Azure Backup and Restore Operations Manual



Azure VM, SQL in VM, and Oracle Backup and Restore Procedures

Contents

[1 Azure Virtual Machine Backup and Restore 4](#_Toc87990602)

[1.1 VM Backup Policies 4](#_Toc87990603)

[1.1.1 DefaultIaaSPolicy 4](#_Toc87990604)

[1.1.2 Create VM Backup Policies 4](#_Toc87990605)

[1.1.3 Edit existing VM Backup Policies 6](#_Toc87990606)

[1.1.4 Assign a VM Backup Policy 10](#_Toc87990607)

[1.2 Backup a Virtual Machine Manually 14](#_Toc87990608)

[1.3 Monitor Backup Job Status 16](#_Toc87990609)

[1.4 Restore a Virtual Machine 17](#_Toc87990610)

[2 Azure SQL in VM Backup and Restore 23](#_Toc87990611)

[2.1 SQL Server in Azure VM Backup Policies 23](#_Toc87990612)

[2.1.1 SQLNonPrdNoTlog 23](#_Toc87990613)

[2.1.2 SQLNonPrdWithTlog 24](#_Toc87990614)

[2.1.3 SQLNonPrd-FullDiffTlog 25](#_Toc87990615)

[2.1.4 SQLPrdNoTlog 26](#_Toc87990616)

[2.1.5 SQLPrdWithTlog 27](#_Toc87990617)

[2.1.6 SQLPrd-FullDiffTlog 28](#_Toc87990618)

[2.1.7 Create SQL Server in Azure VM Backup Policies 28](#_Toc87990619)

[2.1.8 Edit existing SQL Backup Policies 30](#_Toc87990620)

[2.1.9 Assign a SQL Server in Azure VM Backup Policy 32](#_Toc87990621)

[2.2 Back up SQL Server in Azure VM Manually 38](#_Toc87990622)

[2.3 Restore a standalone database from Azure Backup 40](#_Toc87990623)

[2.3.1 Restore to Alternate Location Method 42](#_Toc87990624)

[2.3.2 Restore with Overwrite DB Method 47](#_Toc87990625)

[2.3.3 Restore as Files Method 49](#_Toc87990626)

[2.4 Restore a database belonging to an Always On Availability Group 51](#_Toc87990627)

[2.4.1 Restore to Alternate Location Method 51](#_Toc87990628)

[2.4.2 Restore as Files Method 53](#_Toc87990629)

[3 RMAN Backup and restore 54](#_Toc87990630)

[3.1 RMAN Backup Policies/Scripts 54](#_Toc87990631)

[3.1.1 Full Backup “FULL\_BKP.sh” 54](#_Toc87990632)

[3.1.2 Incremental Backup “INC\_BKP.sh” 56](#_Toc87990633)

[3.1.3 Archive Backup “ARC\_BKP.sh” 57](#_Toc87990634)

[3.2 Database Restoration 59](#_Toc87990635)

[3.2.1 DB Full Backup Restoration 59](#_Toc87990636)

[3.3 Monitoring and Alerts 61](#_Toc87990637)

[3.3.1 Disk Utilisation 61](#_Toc87990638)

[3.3.2 DB Down Alert Report 62](#_Toc87990639)

[3.3.3 Listener Down Alert Report 64](#_Toc87990640)

[3.4 Running backups and Alerts 67](#_Toc87990641)

[3.4.1 Cronjobs 67](#_Toc87990642)

[4 Configuring and Mounting Storage account 69](#_Toc87990643)

[4.1.1 Storage Account and Private Endpoints 69](#_Toc87990644)

[4.1.2 Mounting storage account using “blobfuse” 70](#_Toc87990645)

[5 RMAN Backup Retention Policy 71](#_Toc87990646)

[5.1.1 Storage Account Lifecycle Management 71](#_Toc87990647)

1. Azure Virtual Machine Backup and Restore
   1. VM Backup Policies

The Azure Backup service uses backup policies to manage backup schedules for Azure virtual machines. A default policy has been configured to manage backups for virtual machines within SpinCo and RemainCo.

* + 1. DefaultIaaSPolicy

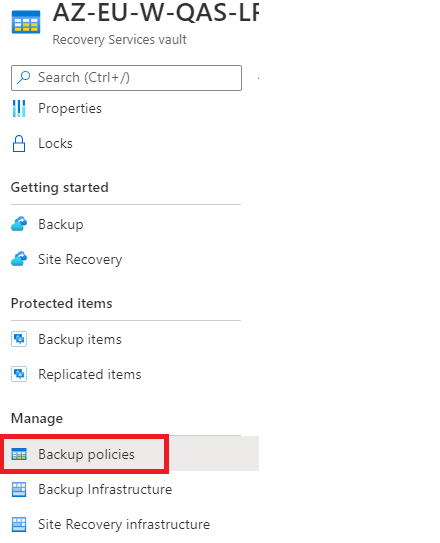
Graphical user interface, text, application, email

Description automatically generated

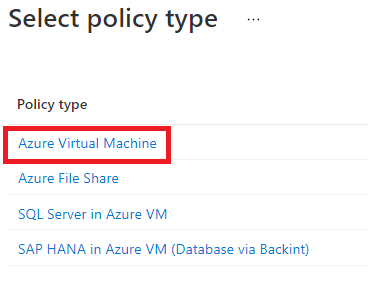
* + 1. Create VM Backup Policies

Backup policies are created, managed, and applied from within a Recovery Services Vault.

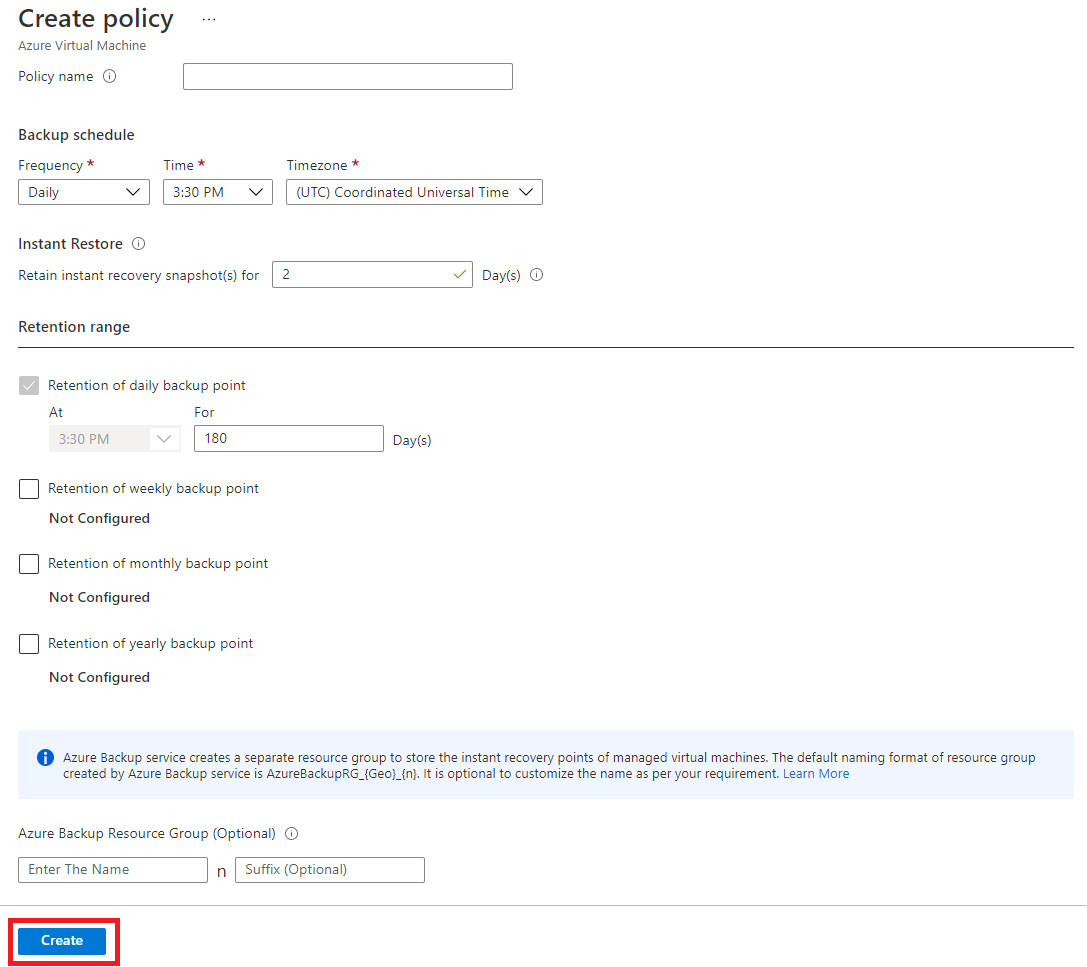
1. Click on Backup policies under the Manage menu item.



1. Click on Add and then Select the Azure Virtual Machine Policy type.

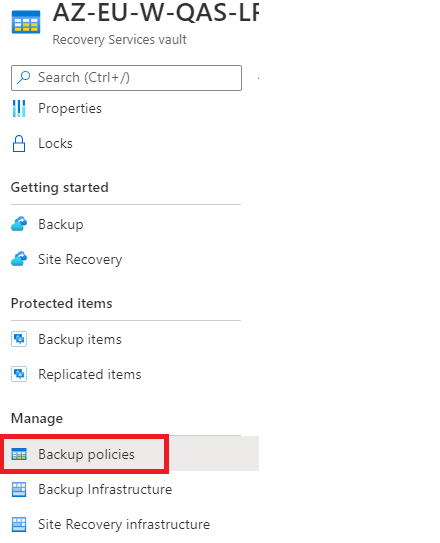


1. Configure the policy and click create.

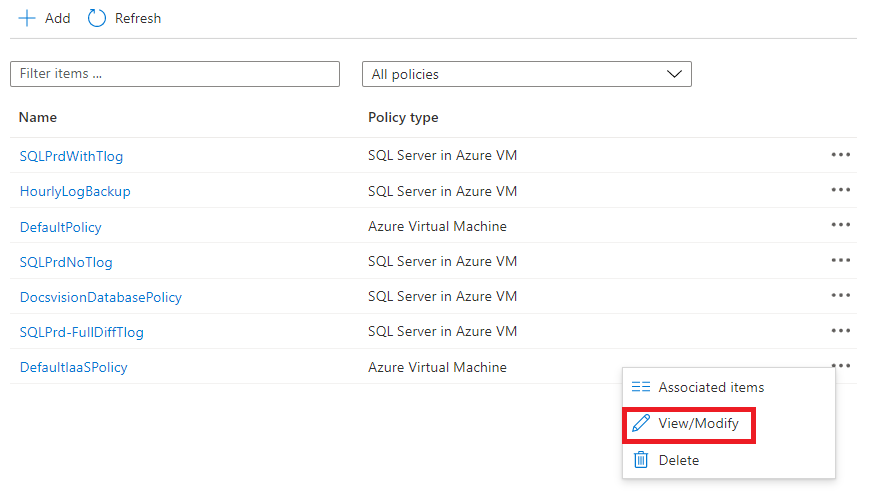


* + 1. Edit existing VM Backup Policies

1. Click on Backup policies under the Manage menu item.

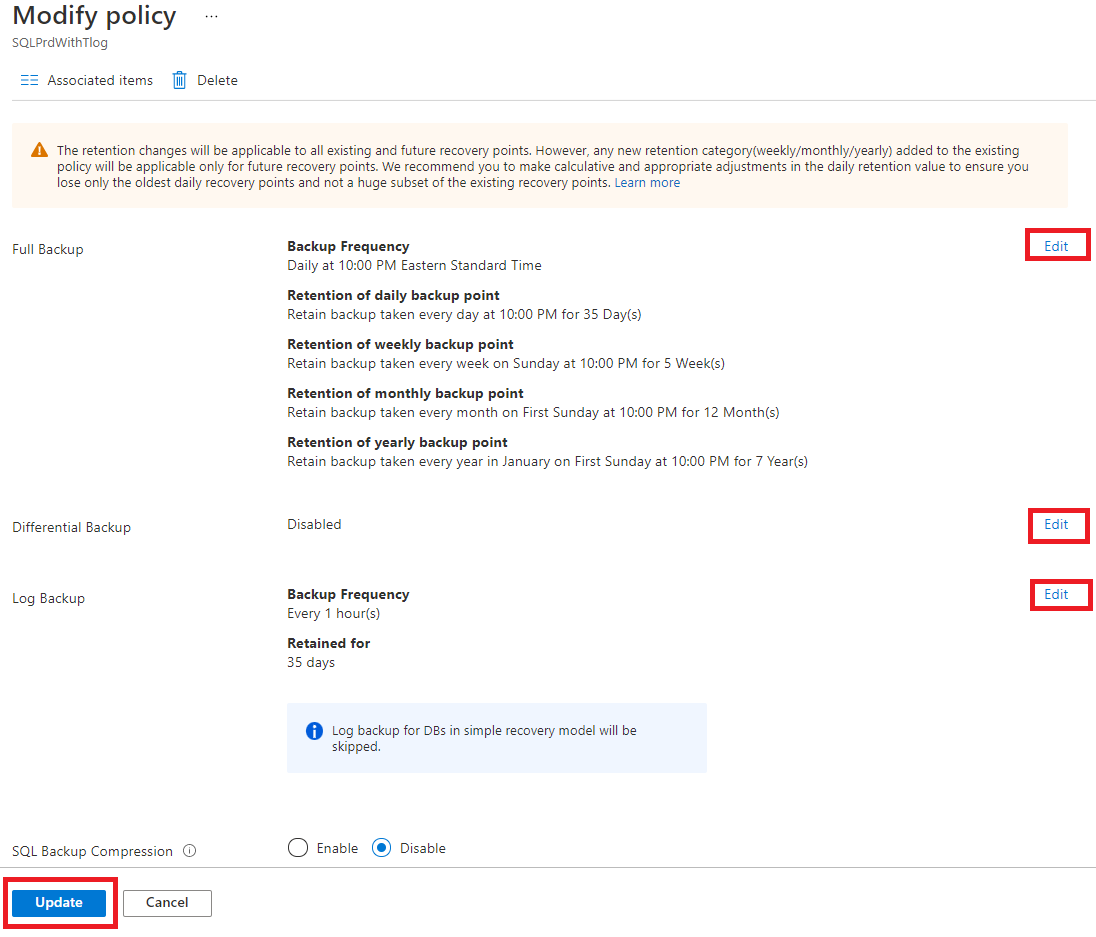


1. Click on the ellipses for the desired policy and select View/Modify.



1. Modify the settings and then click Update.

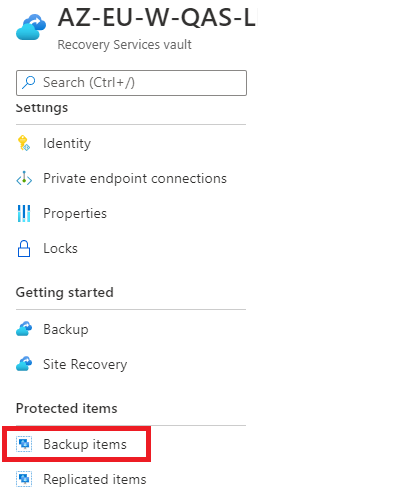




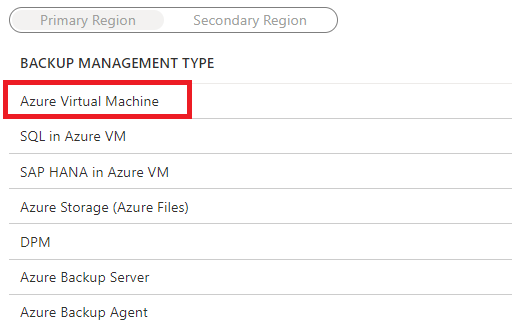
* + 1. Assign a VM Backup Policy

Backup policies should be assigned to virtual machines in the Recovery Services Vault in the same subscription and region as the virtual machine. Select the appropriate recovery services vault and then follow the steps below.

1. Click Backup items under the Protected items menu.



1. Click on Azure Virtual Machine under Backup Management Type.



1. Click on Add.



1. Configure the Backup Goal and click on Backup.



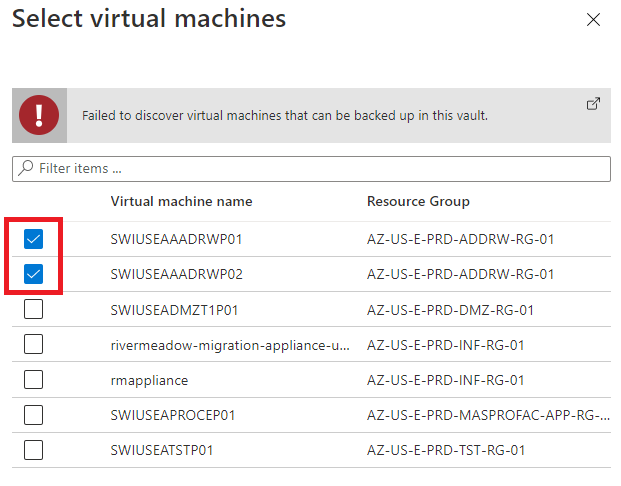
1. Select the Backup policy.

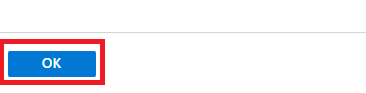
Graphical user interface, text, application

Description automatically generated

1. Click on Add to select the virtual machines to which to apply the policy. On the Select virtual machines pane, check the desired VMs and then click OK.





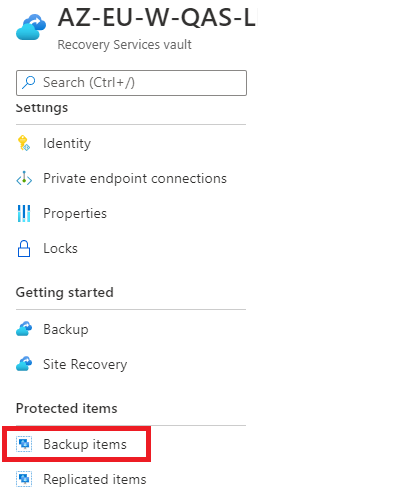


1. Click Enable backup.

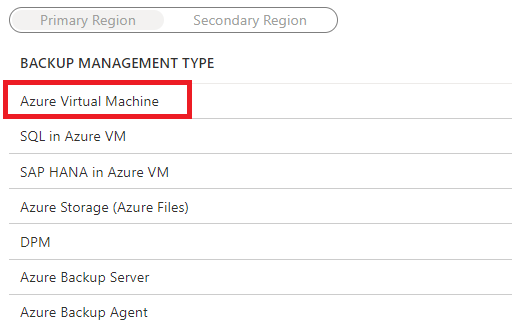


* 1. Backup a Virtual Machine Manually

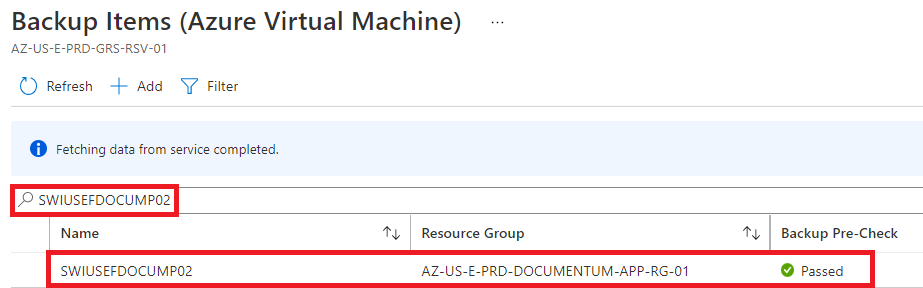
1. Click Backup items under the Getting started menu.



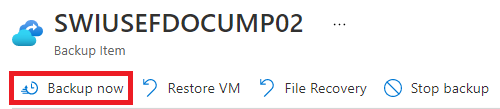
1. Click Azure Virtual Machine under Backup Management Type.



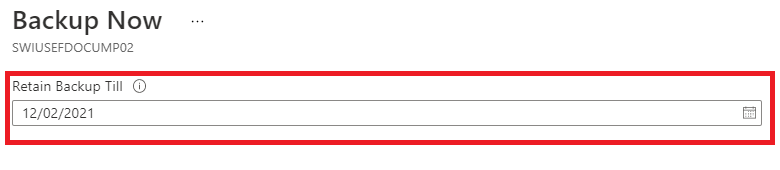
1. Filter the list of Backup items to find the desired virtual machine to backup and then click on the result.



1. Click on Backup now.



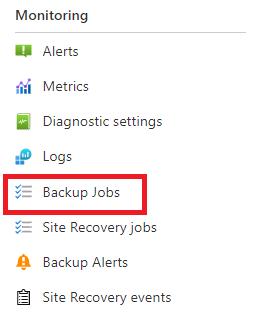
1. Specify a date for the retention of the backup and then click OK.



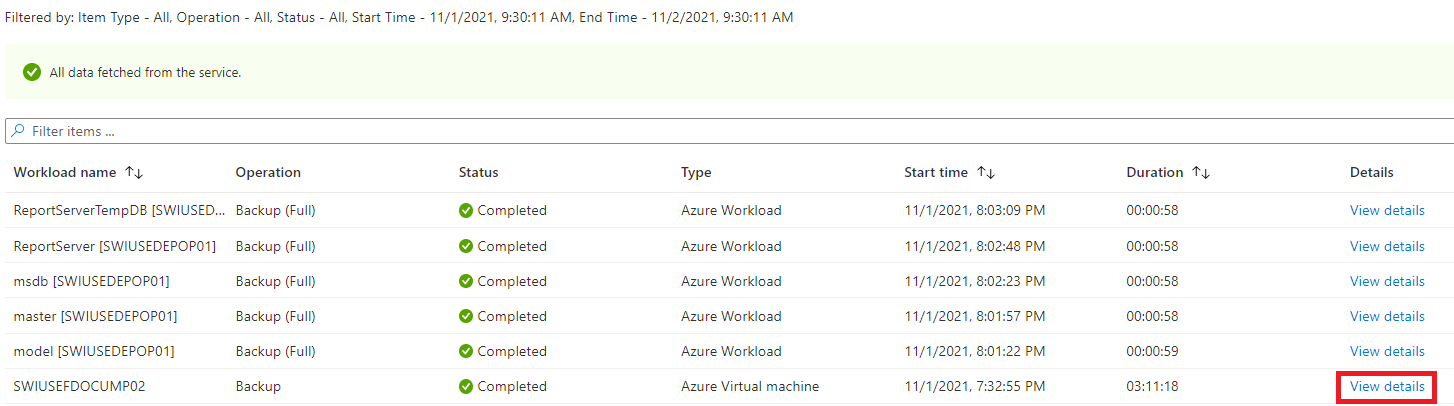


* 1. Monitor Backup Job Status

1. Click Backup Jobs under the Monitoring menu.

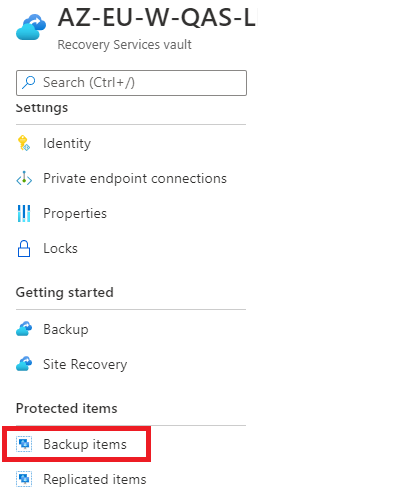


1. Click View details for the desired backup job to view its status.

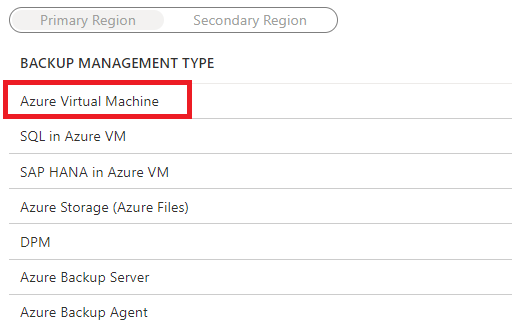


* 1. Restore a Virtual Machine

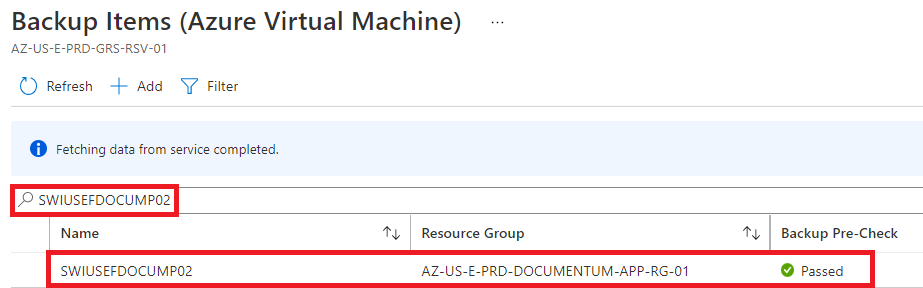
1. Click Backup items under the Protected items menu.



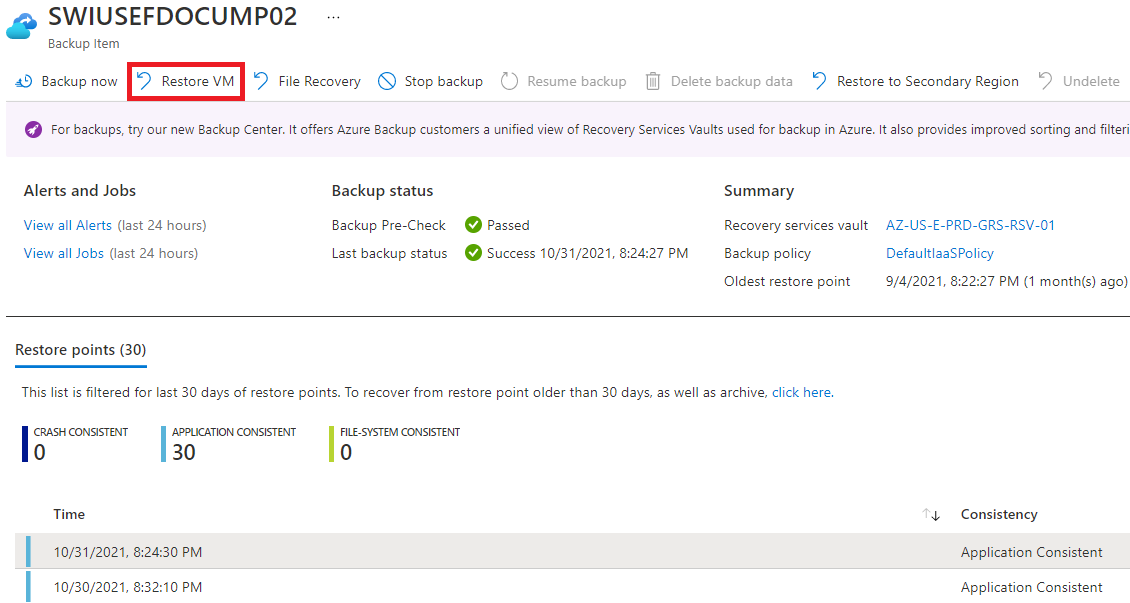
1. Click Azure Virtual Machine under Backup Management Type.



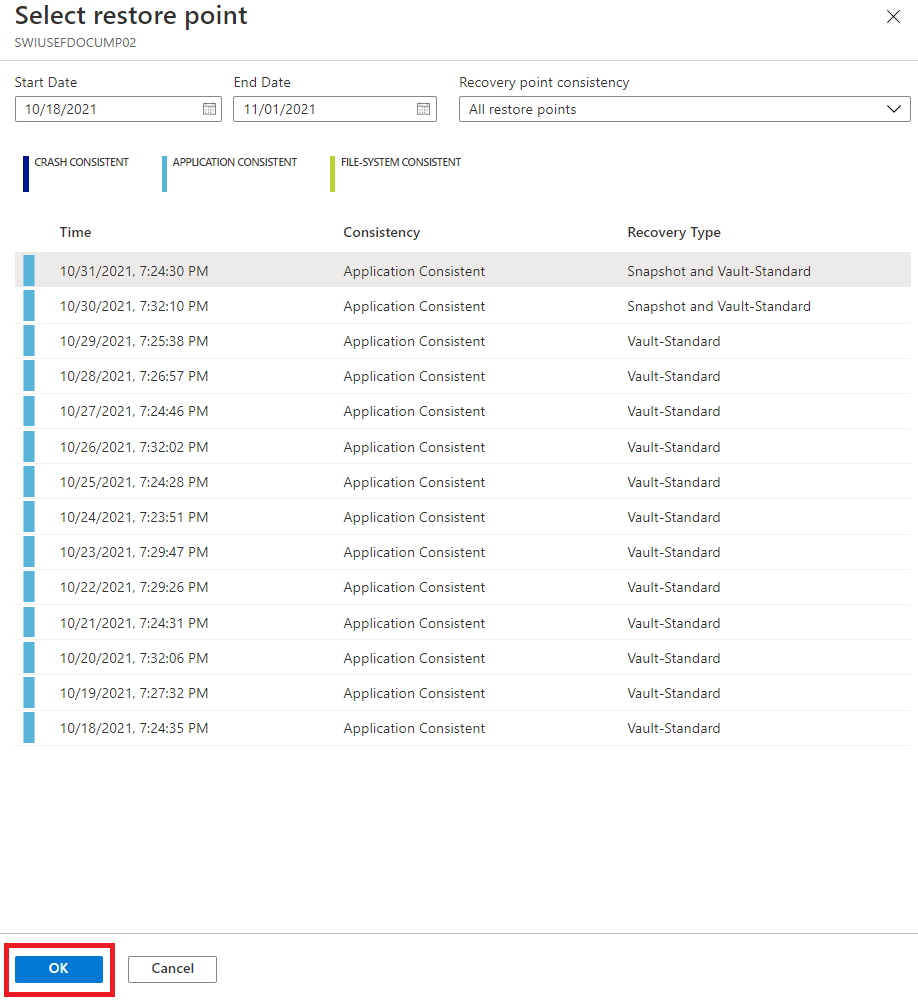
1. Filter the list of Backup items to find the desired virtual machine to restore and then click on the result.



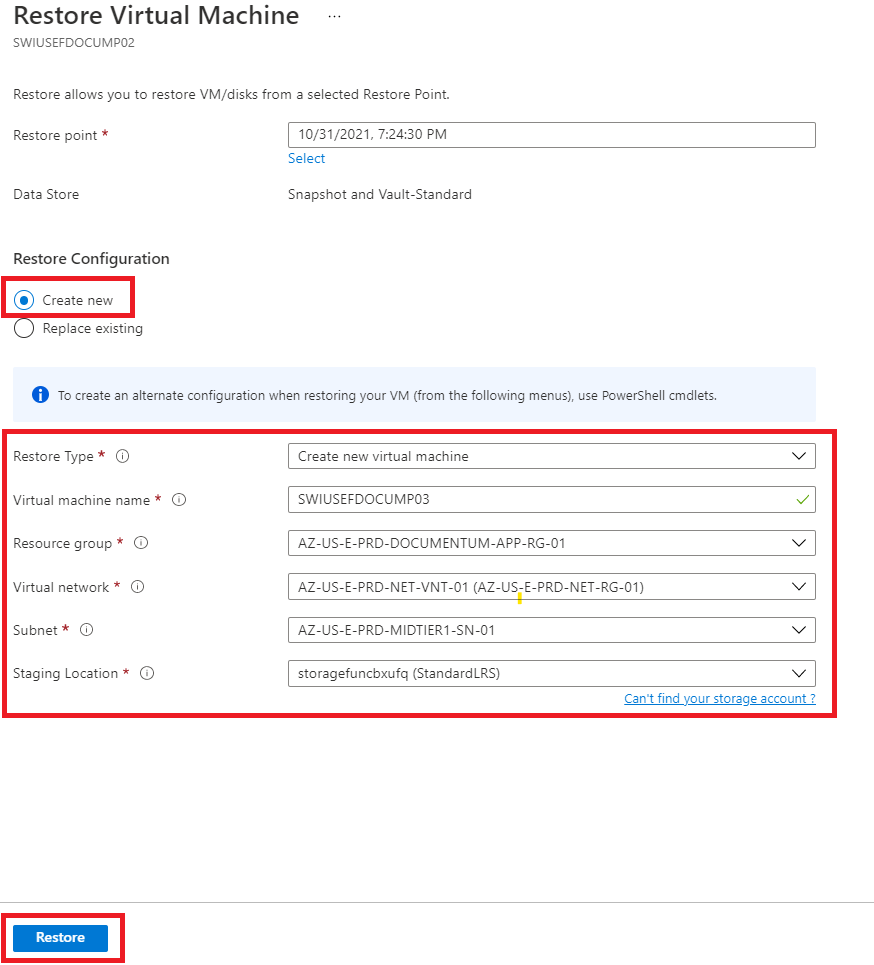
1. Click Restore VM. For information on restore point types, see [Snapshot Consistency](https://docs.microsoft.com/en-us/azure/backup/backup-azure-vms-introduction#snapshot-consistency).

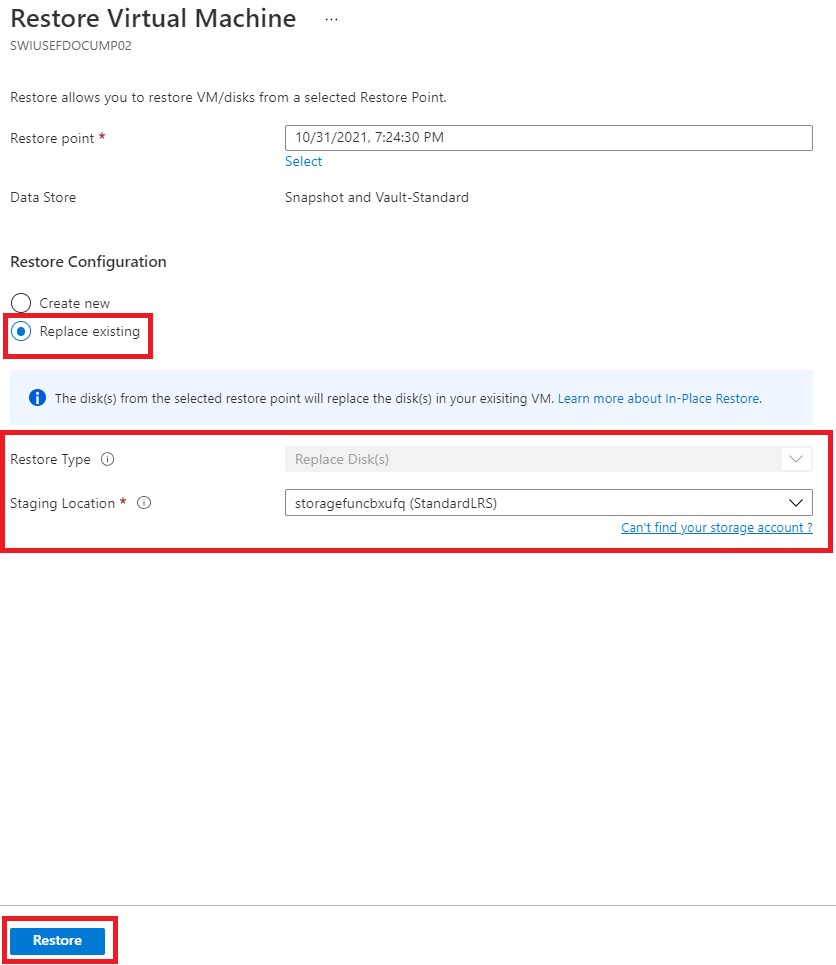


1. Select a restore point and click OK.



1. Select the Restore Configuration and specify the desired settings. A new VM can be created or an existing VM’s disk(s) can be replaced with an In-Place Restore. For more information on Restore Configurations, see [How to restore Azure VM data in the Azure portal](https://docs.microsoft.com/en-us/azure/backup/backup-azure-arm-restore-vms). Finally, click on Restore.





1. Azure SQL in VM Backup and Restore
   1. SQL Server in Azure VM Backup Policies

The Azure Backup service uses backup policies to manage backup schedules and backup types (Full, Differential, and Transaction Logs) for SQL Server in Azure virtual machines. The following policies have been created for non-production and production environments.

* + 1. SQLNonPrdNoTlog

Graphical user interface, text, application

Description automatically generated

* + 1. SQLNonPrdWithTlog

Graphical user interface, text, application, email

Description automatically generated

* + 1. SQLNonPrd-FullDiffTlog

Graphical user interface, text, application, email

Description automatically generated

* + 1. SQLPrdNoTlog

Graphical user interface, text, application, email

Description automatically generated

* + 1. SQLPrdWithTlog

Graphical user interface, text, application, email

Description automatically generated

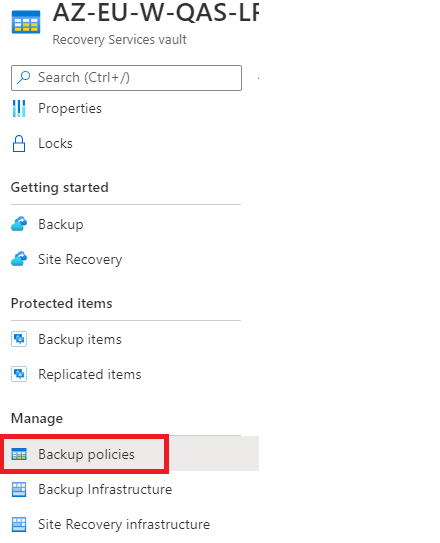
* + 1. SQLPrd-FullDiffTlog

Graphical user interface, text, application

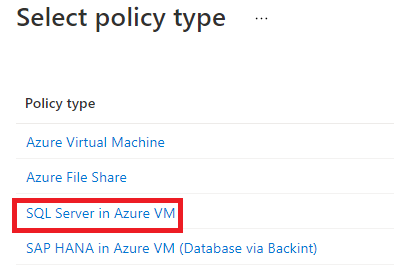
Description automatically generated

* + 1. Create SQL Server in Azure VM Backup Policies

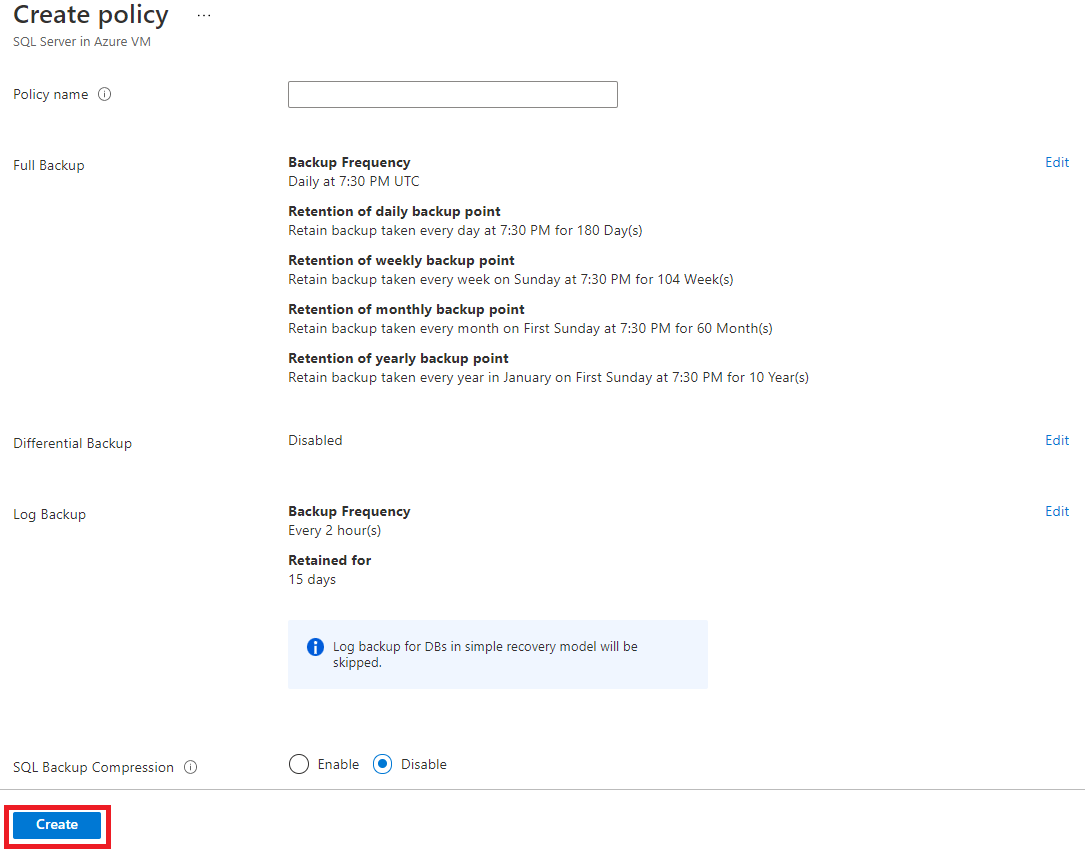
1. Click Backup policies under the Manage menu item.



1. Select the SQL Server in Azure VM policy type.

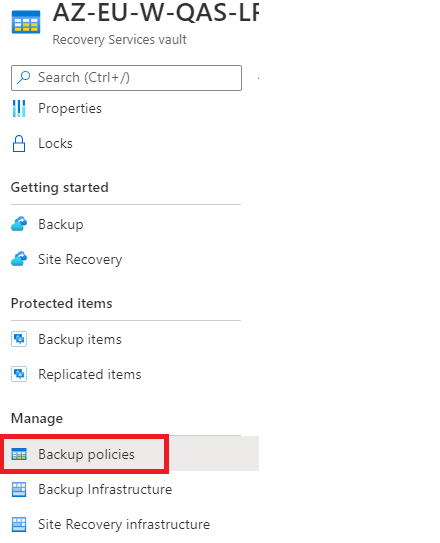


1. Configure the policy and click Create.

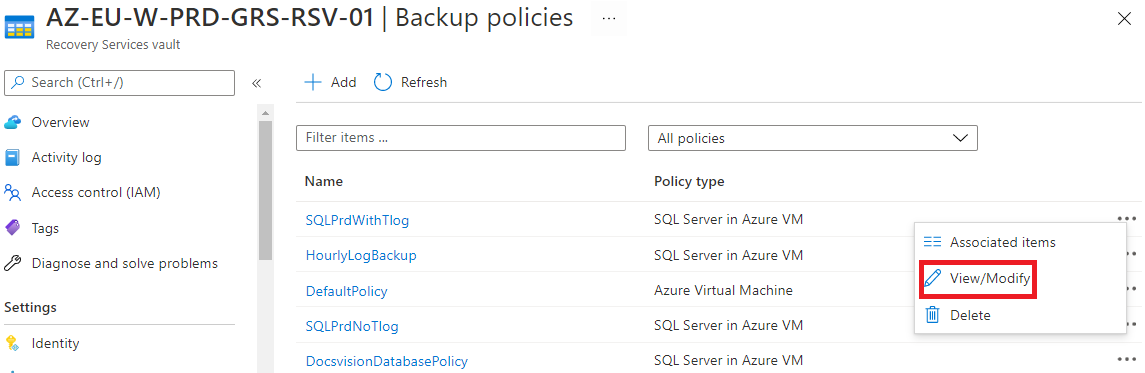


* + 1. Edit existing SQL Backup Policies

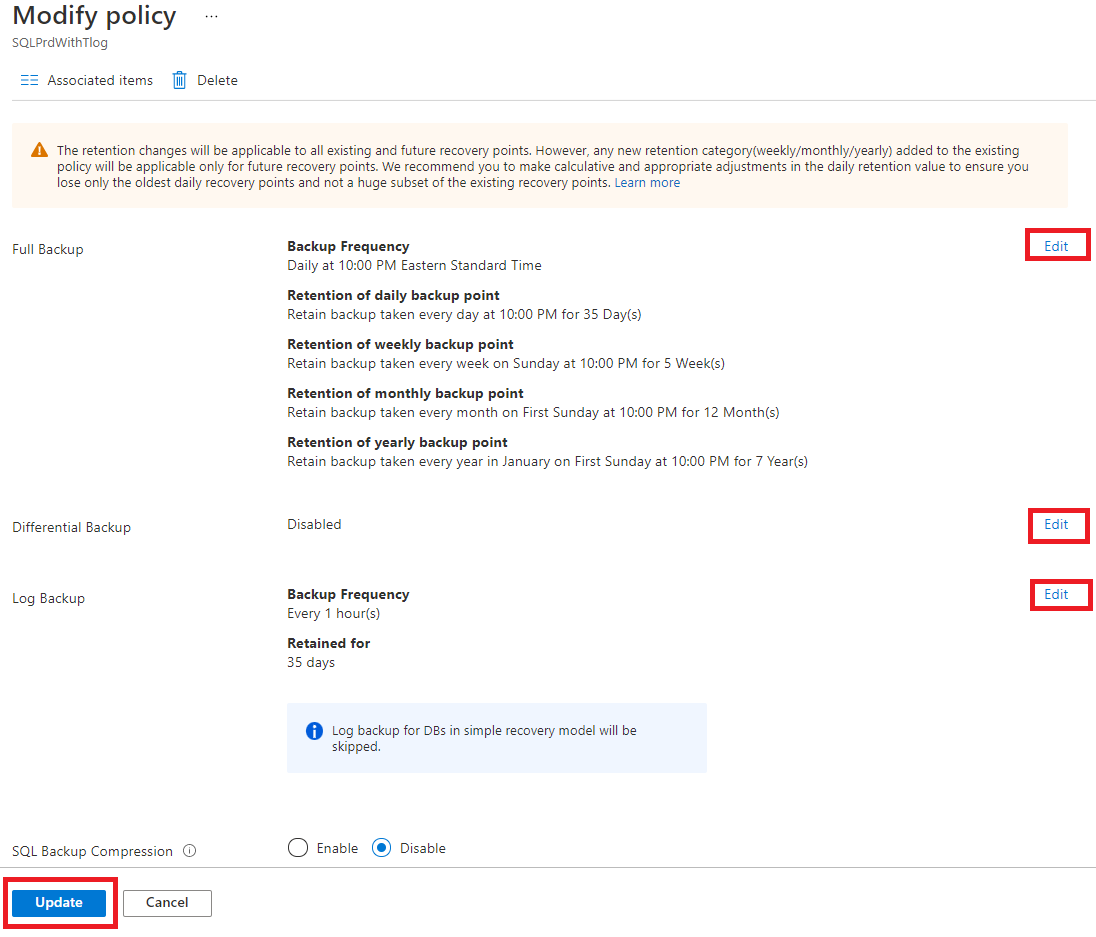
1. Click on Backup policies under the Manage menu item.



1. Click the ellipses for the desired policy and select View/Modify.

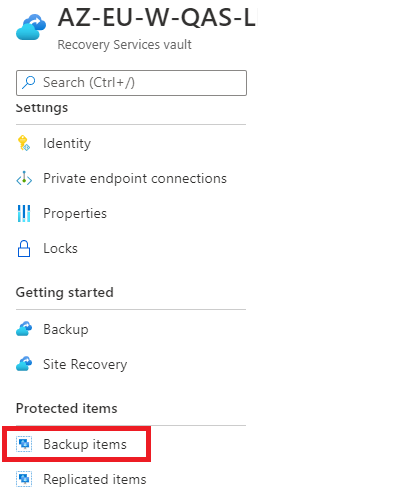


1. Click Edit to modify the settings and then click Update.



* + 1. Assign a SQL Server in Azure VM Backup Policy

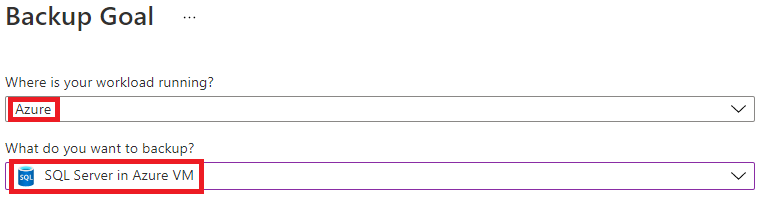
1. Click Backup items under the Protected items menu.



1. Click SQL in Azure VM.



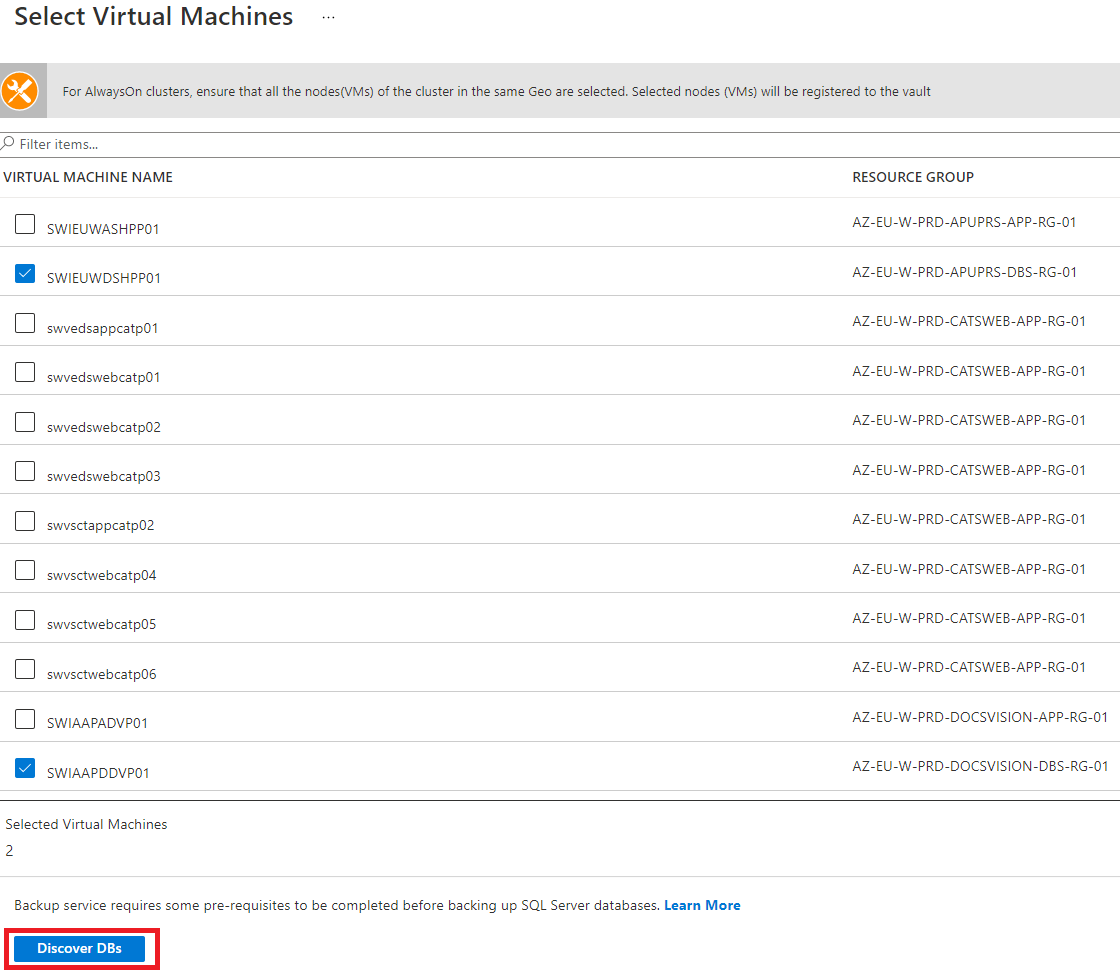
1. Click Add and then configure the Backup Goal, selecting Azure for “Where is your workload running?” and SQL Server in Azure VM for “What do you want to backup?”.



1. Click Start Discovery to discover VMs in the region.

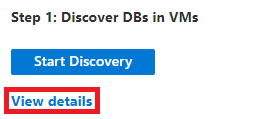


1. Select the VMs for which to Discover databases and click Discover DBs. Selected VMs will be registered with the Recovery Services Vault.



1. During the database discovery process, the Azure Backup service creates a service account “NT Service\AzureWLBackupPluginSvc" that needs SQL sysadmin privileges. If there is an error “UserErrorSQLNoSysadminMembership”, SQL sysadmin privileges must be granted to the service account to obtain a Ready Backup Readiness status. Please see [Setting VM Permissions](https://docs.microsoft.com/en-us/azure/backup/backup-azure-sql-database#set-vm-permissions) for more information.

To view Protected Servers and their Backup Readiness status after the Start Discovery process has been run, Click View Details to display the Protected Servers.



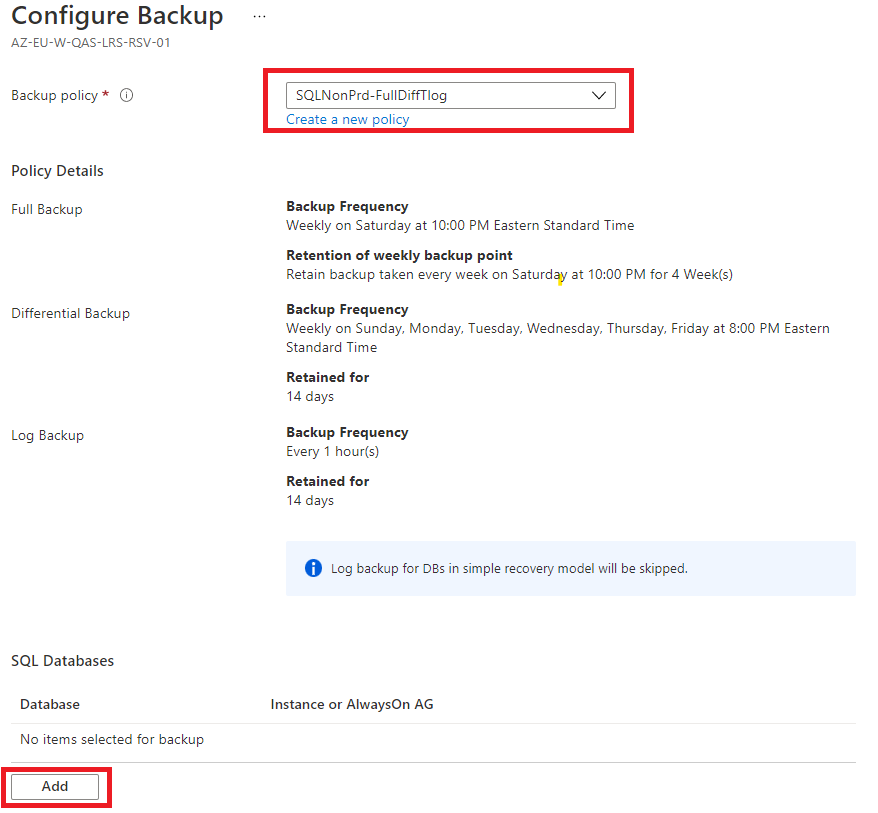
Graphical user interface, text, application

Description automatically generated

1. Once protected servers have a Backup Readiness status of “Ready” with a green check, the backups are ready to be configured. Click Configure Backup to start the configuration process.



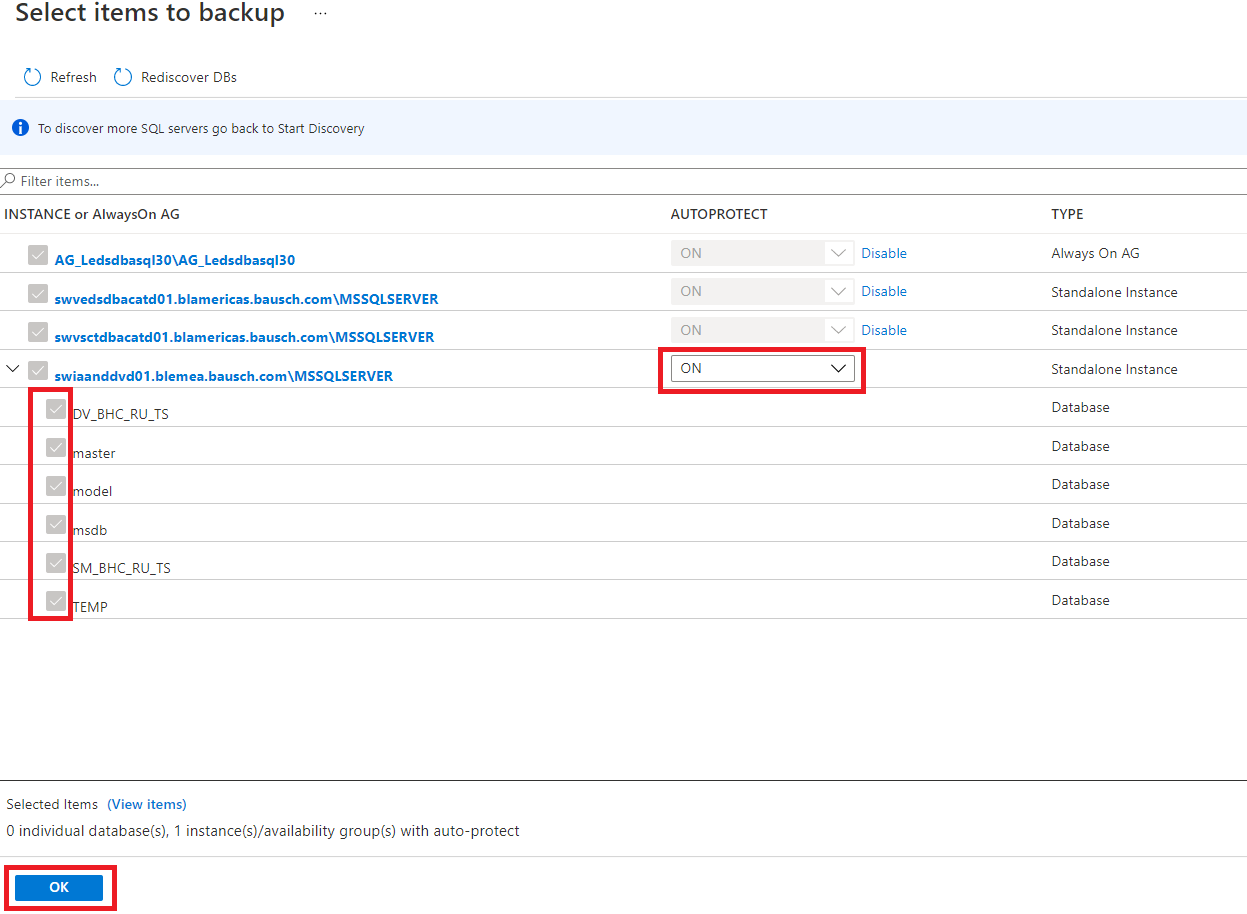
1. Select the desired Backup policy and click Add to select the database instance(s) or AlwaysOn AG(s) to be backed up using the selected policy.



1. In Select items to backup, check the boxes next to the standalone instance(s), database(s), and/or Always On AG(s). Alternatively, under Autoprotect, select ON from the dropdown to automatically select all the databases in the SQL Instance. For more information on Autoprotect, see [Enable auto-protection](https://docs.microsoft.com/en-us/azure/backup/backup-sql-server-database-azure-vms#enable-auto-protection). Once the selections are completed, click OK.

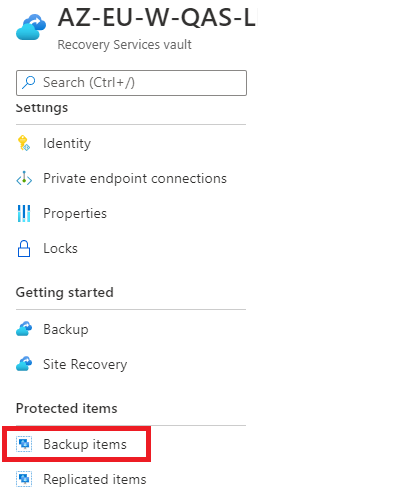
**\*Note**

There are additional considerations for backing up SQL Server Always On Availability Groups such as node backup preference. Please see [Back up SQL Server always on availability groups](https://docs.microsoft.com/en-us/azure/backup/backup-sql-server-on-availability-groups) for more information.

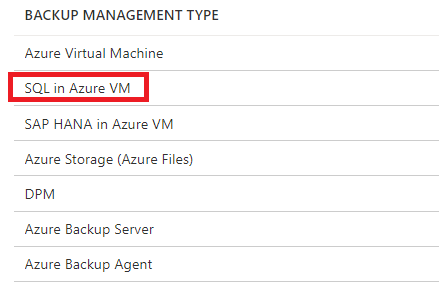


* 1. Back up SQL Server in Azure VM Manually

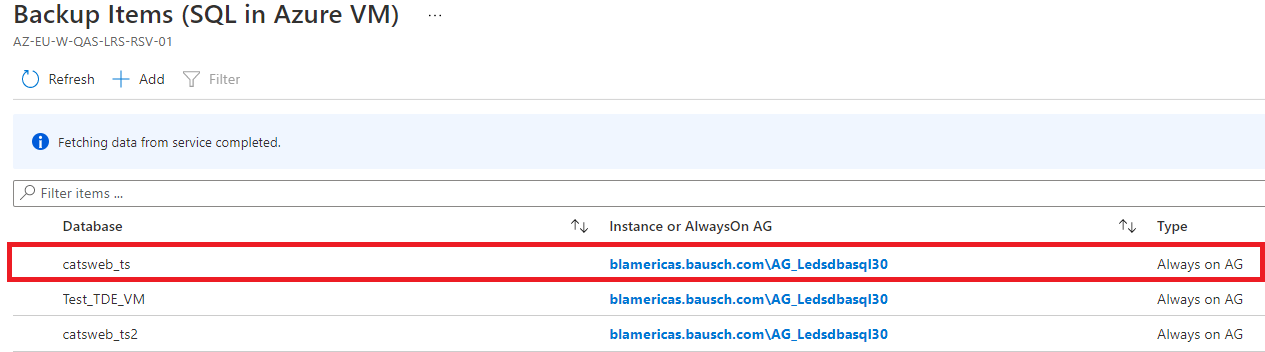
1. Click Backup items under the Protected items menu.



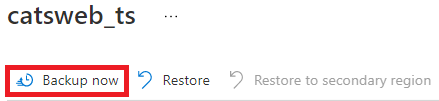
1. Click SQL in Azure VM under Backup Management Type.

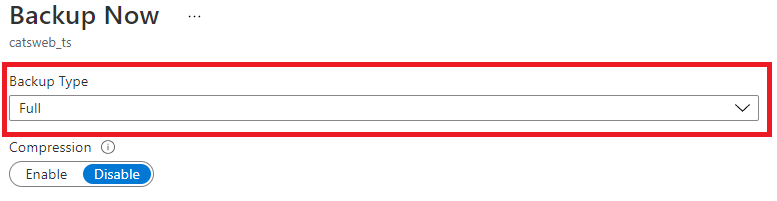


1. Click the desired standalone instance or Always on AG.



1. Click Backup now, select the Backup Type, and click OK.

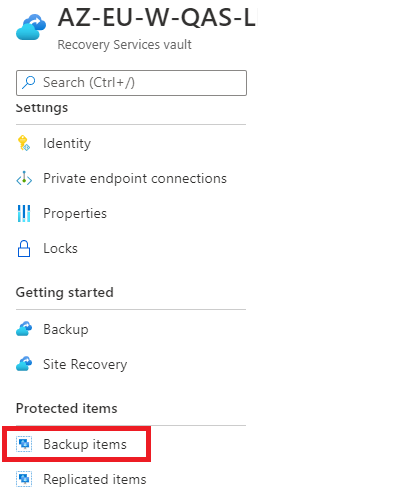




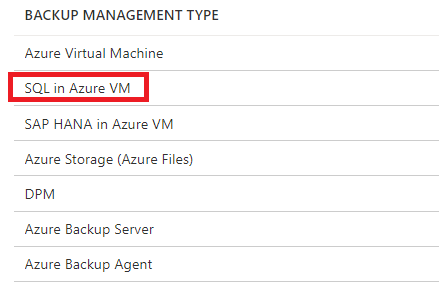


* 1. Restore a standalone database from Azure Backup

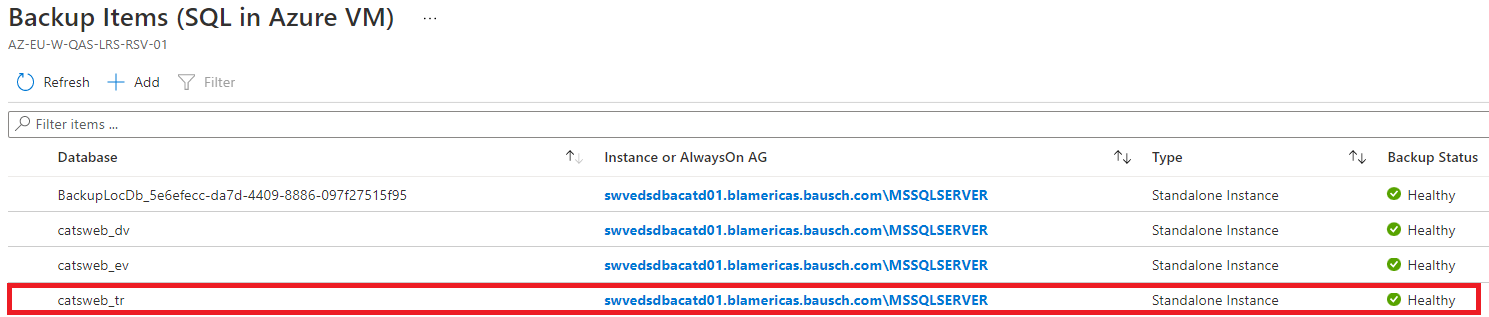
1. Click Backup items under the Protected items menu.



1. Click SQL in Azure VM under Backup Management.



1. Click on the desired standalone instance to restore.

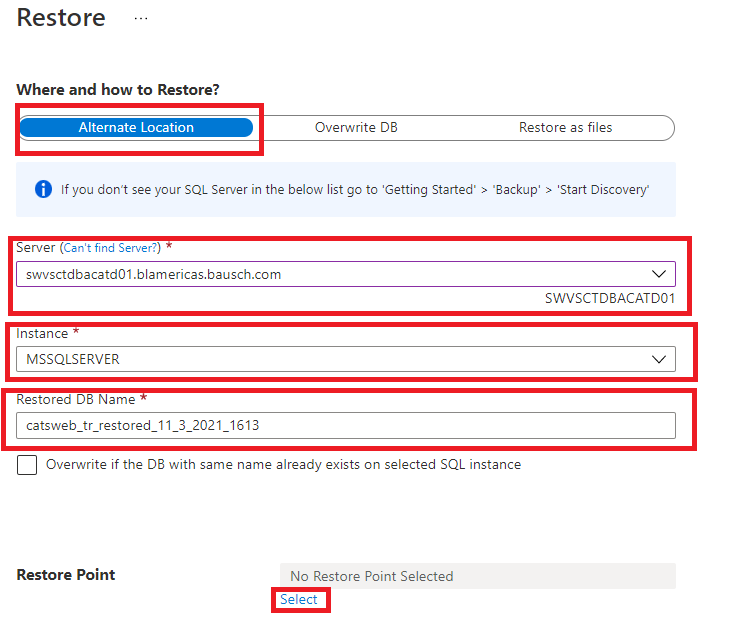


1. Click Restore.



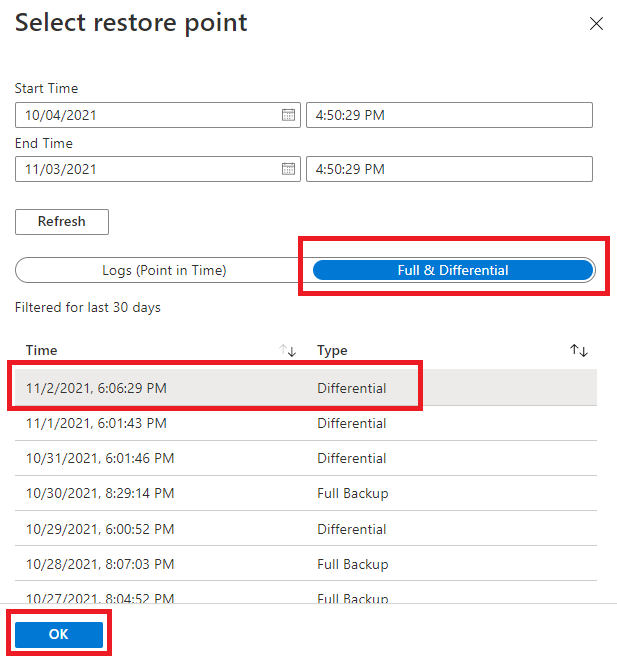
* + 1. Restore to Alternate Location Method

1. Select Alternate Location, select the Server where the database should be restored, select the Instance, and supply the Restored DB Name. Then click Select to select the restore point.



1. On the Select restore point pane, select Logs (Point in Time) for a point in time restore that will restore the corresponding full, differential, and log backups or select Full & Differential to select specific full or differential backups, then click OK.

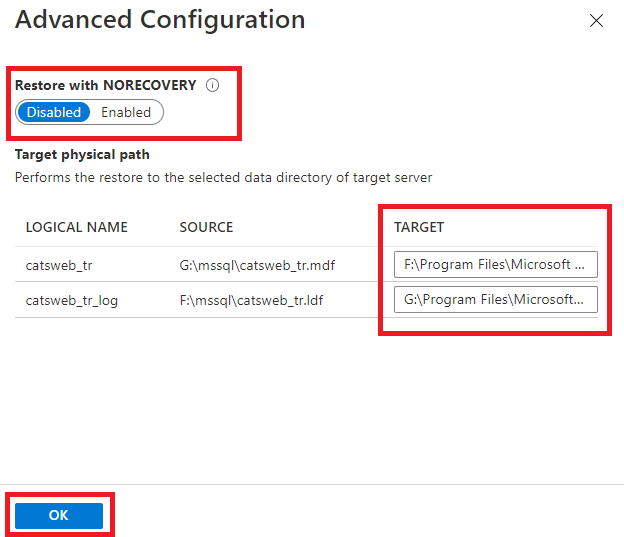


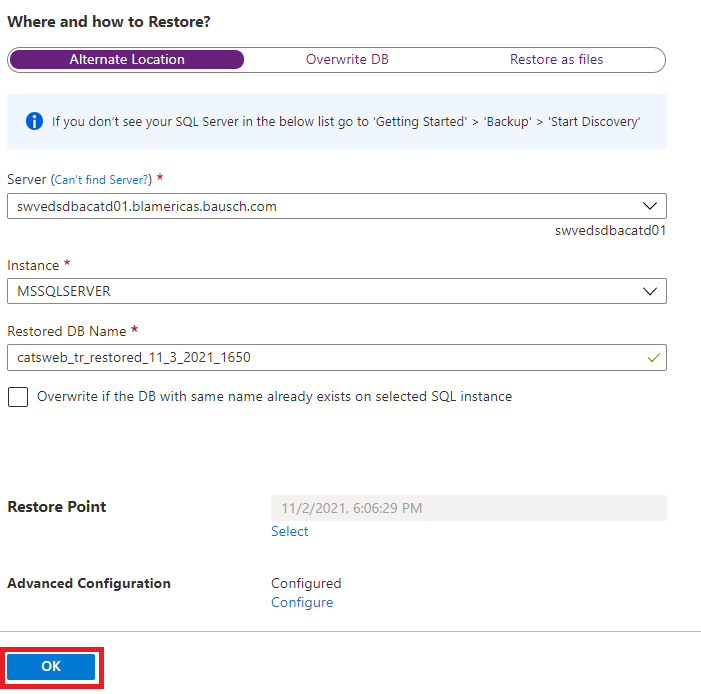


1. Click Configure next to Advanced Configuration.



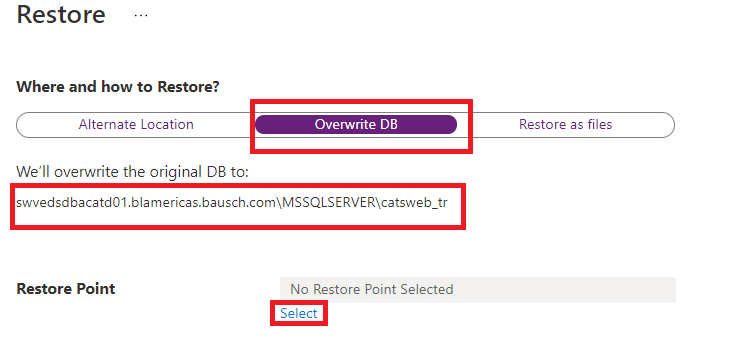
1. On the Advanced Configuration pane, configure the Restore with NoRecovery setting as required and the Target physical path as desired and then click OK.



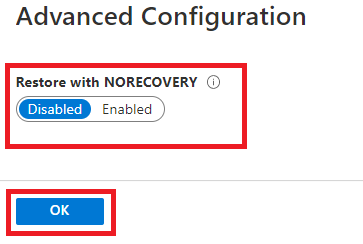
1. Click OK to start the restore job.
2. For more information on this method, see [Restore to an alternate location](https://docs.microsoft.com/en-us/azure/backup/restore-sql-database-azure-vm#restore-to-an-alternate-location).

* + 1. Restore with Overwrite DB Method

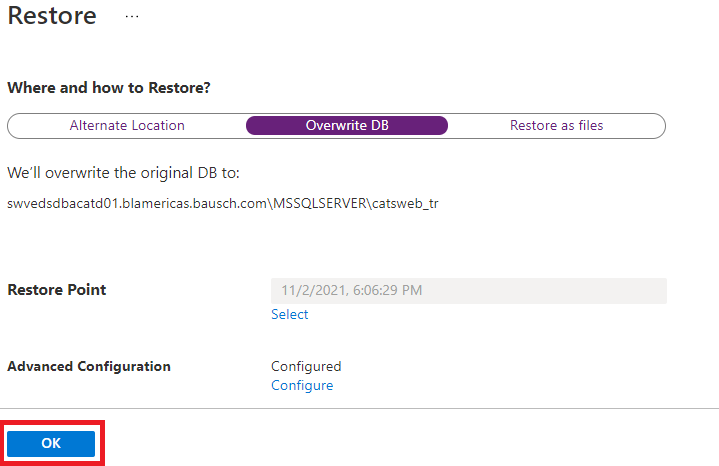
1. Select Overwrite DB, verify the intended location of the database to be overwritten, and then click Select to select a restore point.



1. On the Select restore point pane, select a restore point as described previously in the Alternate Location Method.
2. Click Configure. On the Advanced Configuration pane, configure the Restore with NoRecovery setting as required and click OK.



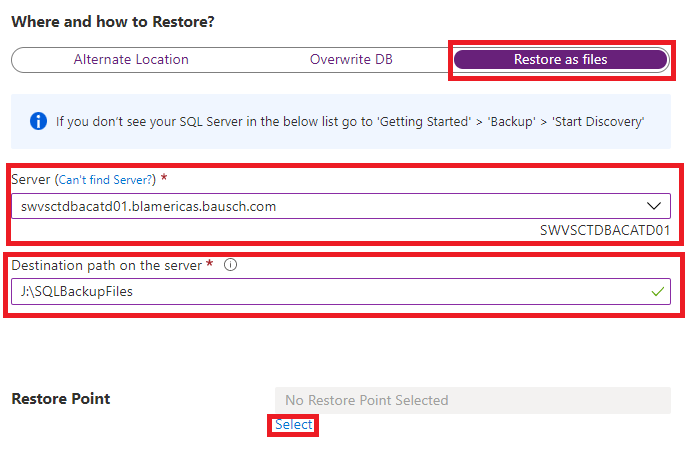
1. Click OK to start the restore job.



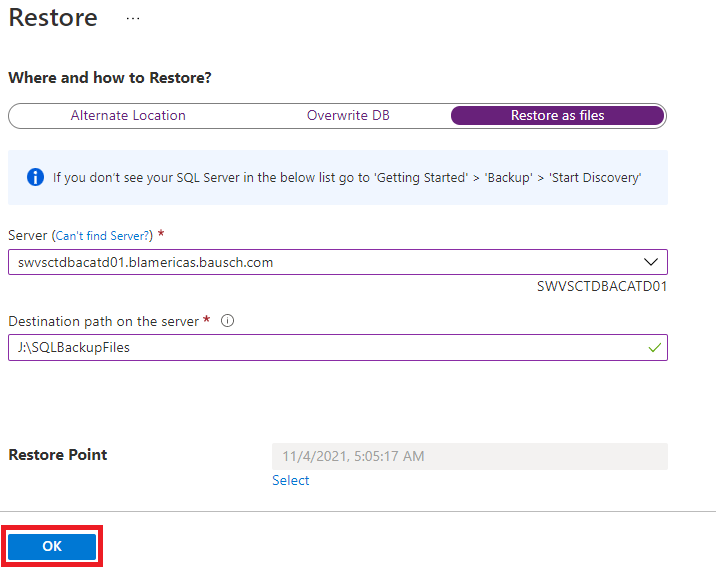
1. For more information on this method, see [Restore and overwrite](https://docs.microsoft.com/en-us/azure/backup/restore-sql-database-azure-vm#restore-and-overwrite).
   * 1. Restore as Files Method

The restore as files method downloads .bak files to a specified location on a server where they can then be copied to any machine and restored as a database. This allows databases to be restored across subscriptions and regions.

1. Select Restore as files, select the Server where the files should be restored, specify the path on the server where the files should be downloaded, and then click Select to choose a restore point.



1. On the Select restore point pane, select a restore point as described previously in the Alternate Location Method.
2. Click Ok to start the restore job.

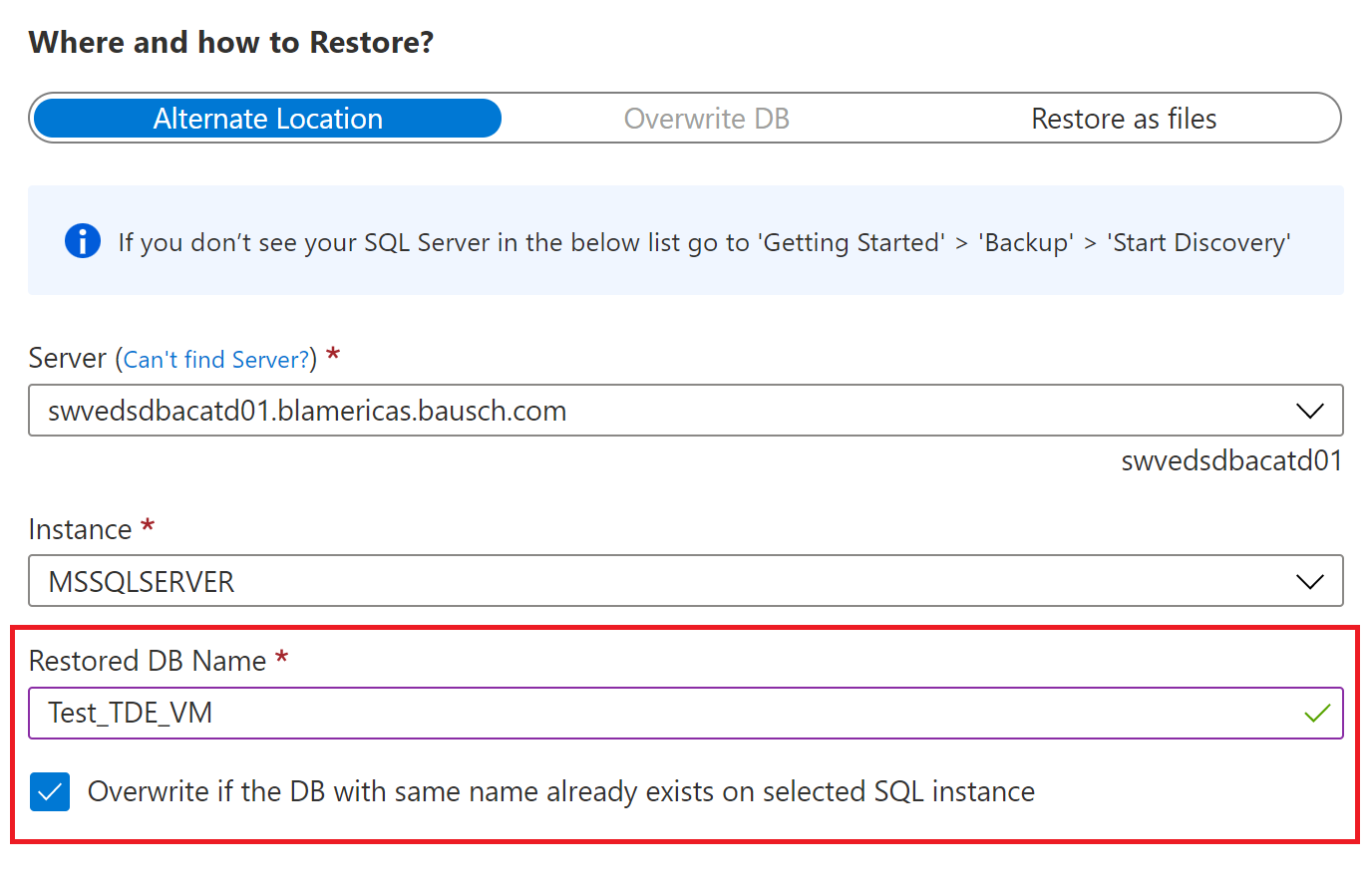


1. For more information on this method, see [Restore as files.](https://docs.microsoft.com/en-us/azure/backup/restore-sql-database-azure-vm#restore-as-files)
   1. Restore a database belonging to an Always On Availability Group

If a database belongs to an Always On availability group, SQL Server doesn’t allow the database to be overwritten. Only Alternate Location and Restore as files methods are available.

* + 1. Restore to Alternate Location Method

1. Remove the database from the availability group via SQL Server Management Studio (SSMS).
2. Take the database offline on the secondary server node via SSMS.
3. Restore the database on the primary node using the Restore to Alternate Location method described in the previous section. It’s possible to overwrite the database once it has been removed from the availability group by specifying the same database name in the Restored DB Name field and checking the Overwrite if the DB with the same name already exists on selected SQL instance option. Alternatively, a different database name can be used. By default, the database will be restored in WITH RECOVERY mode.



1. Restore the database on the secondary node server(s) using the same Restore to Alternate Location method used on the primary node, this time enabling Restore with NORECOVERY on the Advanced Configuration pane.



1. Finally, add the database back into the Availability Group.
   * 1. Restore as Files Method
2. Remove the database from the availability group via SQL Server Management Studio.
3. Take the database offline on the secondary server node via SSMS.
4. Restore the database on the primary node using the Restore as Files method described in the previous section.
5. Restore the database on the secondary node using downloaded backup files from the primary node server or by using the Restore as Files method again to download the files to the secondary node server.
6. Finally, add the database back into the Availability Group.
7. RMAN Backup and restore
   1. RMAN Backup Policies/Scripts

The RMAN backup policies are written in the form of shell scripts and located under “/opt/oracle/scripts”. These scripts are run using cronjobs at different times to take Full, Incremental, Archive backups of the Oracle Database. These scripts are common for both Prod and non-prod.

* + 1. Full Backup “FULL\_BKP.sh”

#!/bin/bash

PATH=/usr/bin:/sbin:/usr/sbin:/bin:/usr/local/bin;export PATH

export ORACLE\_SID=$1

export ORAENV\_ASK=NO

source oraenv

export ORACLE\_HOME=/opt/oracle/product/12.2.0.1/dbhome\_1

export DATE=$(date +%y-%m-%d\_%H%M)

mkdir -p "/rmanbackup/$ORACLE\_SID/FULL/$DATE"

export FULL\_DIR=/rmanbackup/$ORACLE\_SID/FULL/$DATE

mkdir -p "/rmanbackup/$ORACLE\_SID/Archive/$DATE"

export ARC\_DIR=/rmanbackup/$ORACLE\_SID/Archive/$DATE

mkdir -p /rmanbackup/$ORACLE\_SID/Backup\_Log

rman target / log=/rmanbackup/$ORACLE\_SID/Backup\_Log/${ORACLE\_SID}\_FULL\_BACKUP\_${DATE}.log << EOF

run

{

allocate channel d1 type disk format '$FULL\_DIR/${ORACLE\_SID}\_FULL\_backup\_%t\_%s\_%U.bck' maxpiecesize 10240M;

allocate channel d2 type disk format '$FULL\_DIR/${ORACLE\_SID}\_FULL\_backup\_%t\_%s\_%U.bck' maxpiecesize 10240M;

allocate channel d3 type disk format '$FULL\_DIR/${ORACLE\_SID}\_FULL\_backup\_%t\_%s\_%U.bck' maxpiecesize 10240M;

allocate channel d4 type disk format '$FULL\_DIR/${ORACLE\_SID}\_FULL\_backup\_%t\_%s\_%U.bck' maxpiecesize 10240M;

BACKUP INCREMENTAL LEVEL 0 DATABASE;

release channel d1;

release channel d2;

release channel d3;

release channel d4;

allocate channel d5 type disk format '$ARC\_DIR/${ORACLE\_SID}\_ARCH\_backup\_%t\_%s\_%U.bck' maxpiecesize 10240M;

crosscheck archivelog all;

sql 'alter system archive log current';

backup as backupset archivelog all delete input;

backup current controlfile format '$FULL\_DIR/${ORACLE\_SID}\_CONTROL\_backup\_%t\_%s\_%p\_%U.bck';

release channel d5;

}

EOF

export error\_log\_file\_name="/rmanbackup/$ORACLE\_SID/Backup\_Log/${ORACLE\_SID}\_FULL\_BACKUP\_${DATE}.log"

#export DBA\_LIST="mazher.mohammed@bauschhealth.com,abhirup.mukherjee@bauschhealth.com,t.bhuwaneshwari@bauschhealth.com,surendhar.k@bauschhealth.com,shiva.kakkula@bauschhealth.com"

export DBA\_LIST="shiva.kakkula@bauschhealth.com,dl-gbl-oracledbas@bauschhealth.com,Helpdesk@bauschhealth.com"

echo $error\_log\_file\_name

if [ `grep "RMAN-" $error\_log\_file\_name|wc -l` -ge 1 ];

then

mailx -s "$ORACLE\_SID FULL Backup failed" -a $error\_log\_file\_name $DBA\_LIST < $error\_log\_file\_name

fi

* + 1. Incremental Backup “INC\_BKP.sh”

#!/bin/bash

export ORACLE\_SID=$1

export ORAENV\_ASK=NO

. oraenv

#export ORACLE\_HOME=/opt/oracle/product/12.2.0.1/dbhome\_1

export DATE=$(date +%y-%m-%d\_%H%M)

mkdir -p "/rmanbackup/$ORACLE\_SID/INC/$DATE"

export INC\_DIR=/rmanbackup/$ORACLE\_SID/INC/$DATE

mkdir -p "/rmanbackup/$ORACLE\_SID/Archive/$DATE"

export ARC\_DIR=/rmanbackup/$ORACLE\_SID/Archive/$DATE

rman target / log=/rmanbackup/$ORACLE\_SID/Backup\_Log/${ORACLE\_SID}\_INC\_BACKUP\_${DATE}.log << EOF

run

{

allocate channel d1 type disk format '$INC\_DIR/${ORACLE\_SID}\_INC\_backup\_%t\_%s\_%U.bck' maxpiecesize 10240M;

allocate channel d2 type disk format '$INC\_DIR/${ORACLE\_SID}\_INC\_backup\_%t\_%s\_%U.bck' maxpiecesize 10240M;

allocate channel d3 type disk format '$INC\_DIR/${ORACLE\_SID}\_INC\_backup\_%t\_%s\_%U.bck' maxpiecesize 10240M;

allocate channel d4 type disk format '$INC\_DIR/${ORACLE\_SID}\_INC\_backup\_%t\_%s\_%U.bck' maxpiecesize 10240M;

BACKUP INCREMENTAL LEVEL 1 DATABASE;

release channel d1;

release channel d2;

release channel d3;

release channel d4;

allocate channel d5 type disk format '$ARC\_DIR/${ORACLE\_SID}\_ARCH\_backup\_%t\_%s\_%U.bck' maxpiecesize 10240M;

crosscheck archivelog all;

sql 'alter system archive log current';

backup as backupset archivelog all delete input;

backup current controlfile format '$INC\_DIR/${ORACLE\_SID}\_CONTROL\_backup\_%t\_%s\_%p\_%U.bck';

release channel d5;

}

EOF

export error\_log\_file\_name="/rmanbackup/$ORACLE\_SID/Backup\_Log/${ORACLE\_SID}\_INC\_BACKUP\_${DATE}.log"

export DBA\_LIST="mazher.mohammed@bauschhealth.com,abhirup.mukherjee@bauschhealth.com,t.bhuwaneshwari@bauschhealth.com,surendhar.k@bauschhealth.com,shiva.kakkula@bausch

health.com"

echo $error\_log\_file\_name

if [ `grep "RMAN-" $error\_log\_file\_name|wc -l` -ge 1 ];

then

mailx -s "$ORACLE\_SID INC Backup failed" -a $error\_log\_file\_name $DBA\_LIST < $error\_log\_file\_name

fi

* + 1. Archive Backup “ARC\_BKP.sh”

#!/bin/bash

#export ORACLE\_SID=$1

#export ORAENV\_ASK=NO

#. oraenv

#!/bin/bash

PATH=/usr/bin:/sbin:/usr/sbin:/bin:/usr/local/bin;export PATH

export ORACLE\_SID=$1

export ORAENV\_ASK=NO

source oraenv

export ORACLE\_HOME=/opt/oracle/product/12.2.0.1/dbhome\_1

export DATE=$(date +%y-%m-%d\_%H%M)

mkdir -p "/rmanbackup/$ORACLE\_SID/Archive/$DATE"

export ARC\_DIR=/rmanbackup/$ORACLE\_SID/Archive/$DATE

rman target / log=/rmanbackup/$ORACLE\_SID/Backup\_Log/${ORACLE\_SID}\_ARCHIVE\_BACKUP\_${DATE}.log << EOF

run

{

allocate channel d1 type disk format '$ARC\_DIR/${ORACLE\_SID}\_ARCH\_backup\_%t\_%s\_%U.bck' maxpiecesize 10240M;

crosscheck archivelog all;

sql 'alter system archive log current';

backup as backupset archivelog all delete input;

backup current controlfile format '$ARC\_DIR/${ORACLE\_SID}CONTROL\_backup\_%t\_%s\_%p\_%U.bck';

release channel d1;

}

EOF

export error\_log\_file\_name="/rmanbackup/$ORACLE\_SID/Backup\_Log/${ORACLE\_SID}\_ARCHIVE\_BACKUP\_${DATE}.log"

#export DBA\_LIST="mazher.mohammed@bauschhealth.com,abhirup.mukherjee@bauschhealth.com,t.bhuwaneshwari@bauschhealth.com,surendhar.k@bauschhealth.com,shiva.kakkula@bauschhealth.com"

export DBA\_LIST="shiva.kakkula@bauschhealth.com,dl-gbl-oracledbas@bauschhealth.com,Helpdesk@bauschhealth.com"

echo $error\_log\_file\_name

if [ `grep RMAN- $error\_log\_file\_name|wc -l` -ge 1 ];

then

mailx -s "$ORACLE\_SID Archive Log Backup failed" -a $error\_log\_file\_name $DBA\_LIST < $error\_log\_file\_name

fi

* 1. Database Restoration

To do a database restoration, navigate to the backup location, the backup restoration is done through RMAN prompt.

* + 1. DB Full Backup Restoration
    2. Create required directory
    - Control file
    - Data file
    - Audit
    - Redo Log
    - BDUMP
    1. Start the Database using pfile/spfile at NOMOUNT Status.
    2. Restore Controlfile from Backup.

run

{

allocate channel ch1 device type disk;

restore controlfile from '<Control\_file\_backup\_location>';

release channel ch1;

}

* + 1. Change the Database mode from NOMOUNT

SQL> ALTER DATABASE MOUNT;

* + 1. Start Restore Database.

Add the following parameter to RMAN restore, for restoring the DB to a new path.

set echo off pages 0 feed off sqlp #

spool /path/setnewnamedf.lst

select 'set newname for datafile '||file#||' to NEW;' from v$datafile;

-- select 'set newname for datafile '||file#||' to /newpath/NEW;' from v$datafile;

spool off

run

{

set newname for datafile 1 to '<newpath>';

set newname for datafile 2 to '<newpath>';

set newname for datafile 3 to '<newpath>';

set newname for datafile 4 to '<newpath>';

set newname for datafile 5 to '<newpath>';

set newname for logfile 1 to ‘< Newpath > ‘;

SWITCH DATAFILE ALL;

RESTORE DATABASE;

}

Restoring DB to existing path:

run

{

set datafile 1 to '<path>';

set datafile 2 to '<path>';

set datafile 3 to '<path>';

set datafile 4 to '<path>';

set datafile 5 to '<path>';

set logfile 1 to ‘< path > ‘;

SWITCH DATAFILE ALL;

RESTORE DATABASE;

}

* + 1. Now we need to Recover the Database.

run

{

RECOVER DATABASE;

}

* + 1. Now open the database.

SQL> ALTER DATABASE OPEN RESETLOGS;

* + 1. Now Configure TNSNAME and LISTENER for New Database and also create spfile
  1. Monitoring and Alerts

The alerts are written in the form of scripts (shell scripts) and configured to run as cronjobs. The scripts are located under “/opt/workspace”

* + 1. Disk Utilisation

Disk Utilisation alert triggers when the disk util is more than 85 percent.

1. Disk Utilisation “Disk\_util.sh”

#!/bin/bash

echo -e "Helpdesk,\n\nPlease create and assign a ticket with below description to oracle DBA team. SNOW Group ID: IT Support - Database (Oracle).\n\n" >/opt/workspace/current\_util.log

df -h|head -1 >>/opt/workspace/current\_util.log

df -h|while read line;

do

if [[ `echo $line|grep -viE "/opt$"|awk '{printf "%d", $5}'` -ge 85 ]];

#if any mount point is to be removed from monitoring then please updated above like 'echo $line|grep -viE "mountpoint1$|mountpoint2$"|awk...'

then

echo "$line" >>/opt/workspace/current\_util.log;

fi

done

export DBA\_LIST="shiva.kakkula@bauschhealth.com,dl-gbl-oracledbas@bauschhealth.com,Helpdesk@bauschhealth.com"

#export DBA\_LIST="mazher.mohammed@bauschhealth.com"

if [ `cat /opt/workspace/current\_util.log|wc -l` -ge 7 ];

then

mailx -s "Disk util is high on `hostname`!!!" $DBA\_LIST < /opt/workspace/current\_util.log

fi

#>/opt/workspace/current\_util.log

* + 1. DB Down Alert Report

The DB down alert scripts are located under “/opt/workspace/db\_down\_script\_donotdelete” and alerts are achieved through two scripts.

1. DB instance status “ckinstance\_status\_sliusedorasq50.ksh” (checks the status of the DBs and writes a status log onto “all\_db\_down\_alert.log”)

#!/bin/ksh

##################################################################

## ckinstance\_status\_sliusedorasq50.ksh ##

###################################################################

#DBALIST="shiva.kakkula@bauschhealth.com,DL-USA-OracleDBAs@bauschhealth.com,william.connaughton@bauschhealth.com,Meghana.Dixit@bauschhealth.com";export DBALIST

#DBALIST="shiva.kakkula@bauschhealth.com";export DBALIST

ORATAB=/opt/workspace/db\_down\_script\_donotdelete/temp\_oratab

#export smtp="smtp.bausch.com:25"

echo "`date` "

echo "Oracle Database(s) Status `hostname` :\n"

rm /opt/workspace/db\_down\_script\_donotdelete/sliusedorasq50\_db\_down\_report.txt

touch /opt/workspace/db\_down\_script\_donotdelete/sliusedorasq50\_db\_down\_report.txt

rm /opt/workspace/db\_down\_script\_donotdelete/sliusedorasq50\_db\_up\_report.txt

touch /opt/workspace/db\_down\_script\_donotdelete/sliusedorasq50\_db\_up\_report.txt

touch /opt/workspace/db\_down\_script\_donotdelete/all\_db\_down\_alert.log

echo "Please create and assign a ticket with below description to oracle DBA team. SNOW Group ID: IT Support - Database (Oracle)" >> /opt/workspace/db\_down\_script\_donotdelete/all\_db\_down\_alert.log

echo " " >> /opt/workspace/db\_down\_script\_donotdelete/all\_db\_down\_alert.log

db=`egrep -i ":Y|:N" $ORATAB | cut -d":" -f1 | grep -v "\#" | grep -v "\\*"`

pslist="`ps -ef | grep pmon`"

for i in $db ; do

echo "$pslist" | grep "ora\_pmon\_$i"

if (( $? )); then

echo "Host: sliusedorasq50, Oracle Instance - $i: Down" >> /opt/workspace/db\_down\_script\_donotdelete/sliusedorasq50\_db\_down\_report.txt

else

echo "Host: sliusedorasq50, Oracle Instance - $i: Up" >> /opt/workspace/db\_down\_script\_donotdelete/sliusedorasq50\_db\_up\_report.txt

fi

done

cat /opt/workspace/db\_down\_script\_donotdelete/sliusedorasq50\_db\_down\_report.txt >> /opt/workspace/db\_down\_script\_donotdelete/all\_db\_down\_alert.log

1. Email Alerts “all\_db\_down\_alert\_email.ksh” (sends email alerts based on “all\_db\_down\_alert.log”)

#!/bin/ksh

##################################################################

## all\_db\_down\_alert\_email.ksh ##

###################################################################

export DBALIST="shiva.kakkula@bauschhealth.com,DL-USA-OracleDBAs@bauschhealth.com,william.connaughton@bauschhealth.com,Meghana.Dixit@bauschhealth.com,Helpdesk@bauschhealth.com,"

#export DBALIST="mazher.mohammed@bauschhealth.com"

#DBALIST="shiva.kakkula@bauschhealth.com,DL-USA-OracleDBAs@bauschhealth.com,william.connaughton@bauschhealth.com,Meghana.Dixit@bauschhealth.com";export DBALIST

#DBALIST="shiva.kakkula@bauschhealth.com";export DBALIST

#export smtp="smtp.bausch.com:25"

#### Sleep for 4 minutes and proceed to with below steps ####

sleep 30

#### All DB Outage details for Server ####

file1=/opt/workspace/db\_down\_script\_donotdelete/all\_db\_down\_alert.log

count=`cat ${file1} |grep Host |wc -l`

if [ $count -gt 0 ] ; then

mailx -s "All Database(s) down alert email: " $DBALIST < $file1

fi

rm /opt/workspace/db\_down\_script\_donotdelete/all\_db\_down\_alert.log

* + 1. Listener Down Alert Report

The Listener down scripts are located under “/opt/workspace/listener\_down\_script\_donotdelete/” and the alerts are achieved with two scripts.

1. listener\_status\_sliusedorasq50.ksh (checks the status of the database listeners and writes a status log onto “all\_listener\_down\_alert.log”)

#!/bin/ksh

##################################################################

## ckinstance\_status\_sliusedorasq50.ksh ##

###################################################################

#DBALIST="shiva.kakkula@bauschhealth.com,DL-USA-OracleDBAs@bauschhealth.com,william.connaughton@bauschhealth.com,Meghana.Dixit@bauschhealth.com";export DBALIST

#DBALIST="shiva.kakkula@bauschhealth.com";export DBALIST

ORATAB=/opt/workspace/listener\_down\_script\_donotdelete/temp\_oratab

#export smtp="smtp.bausch.com:25"

echo "`date` "

echo "Oracle Listener(s) Status `hostname` :\n"

rm /opt/workspace/listener\_down\_script\_donotdelete/sliusedorasq50\_listener\_down\_report.txt

touch /opt/workspace/listener\_down\_script\_donotdelete/sliusedorasq50\_listener\_down\_report.txt

rm /opt/workspace/listener\_down\_script\_donotdelete/sliusedorasq50\_listener\_up\_report.txt

touch /opt/workspace/listener\_down\_script\_donotdelete/sliusedorasq50\_listener\_up\_report.txt

touch /opt/workspace/listener\_down\_script\_donotdelete/all\_listener\_down\_alert.log

echo "Please create and assign a ticket with below description to oracle DBA team. SNOW Group ID: IT Support - Database (Oracle)" >> /opt/workspace/listener\_down\_script\_donotdelete/all\_listener\_down\_alert.log

echo " " >> /opt/workspace/listener\_down\_script\_donotdelete/all\_listener\_down\_alert.log

db=`egrep -i ":Y|:N" $ORATAB | cut -d":" -f1 | grep -v "\#" | grep -v "\\*"`

#pslist="`ps -ef | grep pmon`"

pslist="`ps -ef | grep list`"

for i in $db ; do

#tnsping $i >/dev/null

echo "$pslist" | grep "list$i"

if (( $? )); then

echo "Host: sliusedorasq50, Oracle listener - $i: Down" >> /opt/workspace/listener\_down\_script\_donotdelete/sliusedorasq50\_listener\_down\_report.txt

else

echo "Host: sliusedorasq50, Oracle listener - $i: Up" >> /opt/workspace/listener\_down\_script\_donotdelete/sliusedorasq50\_listener\_up\_report.txt

fi

done

cat /opt/workspace/listener\_down\_script\_donotdelete/sliusedorasq50\_listener\_down\_report.txt >> /opt/workspace/listener\_down\_script\_donotdelete/all\_listener\_down\_alert.log

1. Email Alerts “all\_listener\_down\_alert\_email.ksh” (sends email alerts based on “all\_listener\_down\_alert.log”)

#!/bin/ksh

##################################################################

## all\_listener\_down\_alert\_email.ksh ##

###################################################################

#export DBALIST="shiva.kakkula@bauschhealth.com,DL-USA-OracleDBAs@bauschhealth.com,william.connaughton@bauschhealth.com,Meghana.Dixit@bauschhealth.com,Helpdesk@bauschhealth.com,"

export DBALIST="mazher.mohammed@bauschhealth.com,shiva.kakkula@bauschhealth.com,t.bhuwaneshwari@bauschhealth.com"

#DBALIST="shiva.kakkula@bauschhealth.com,DL-USA-OracleDBAs@bauschhealth.com,william.connaughton@bauschhealth.com,Meghana.Dixit@bauschhealth.com";export DBALIST

#DBALIST="shiva.kakkula@bauschhealth.com";export DBALIST

#export smtp="smtp.bausch.com:25"

#### Sleep for 4 minutes and proceed to with below steps ####

sleep 30

#### All DB Outage details for Server ####

file1=/opt/workspace/listener\_down\_script\_donotdelete/all\_listener\_down\_alert.log

count=`cat ${file1} |grep Host |wc -l`

if [ $count -gt 0 ] ; then

mailx -s "All Listener(s) down alert email: " $DBALIST < $file1

fi

rm /opt/workspace/listener\_down\_script\_donotdelete/all\_listener\_down\_alert.log

* 1. Running backups and Alerts

The backup scripts and alert scripts are run as cronjobs. The scripts are run at a specific time against each database.

* + 1. Cronjobs

#crontab -u oracle -l

#\* \* \* \* \* mailx -s "Testing" mazher.mohammed@bauschhealth.com </etc/oratab

###########DISK UTILISATION############

\*/10 \* \* \* \* sh /opt/workspace/disk\_util.sh

######## DB Down Alert Report ##############################

\*/10 \* \* \* \* /opt/workspace/db\_down\_script\_donotdelete/ckinstance\_status\_sliusedorasq50.ksh

\*/10 \* \* \* \* /opt/workspace/db\_down\_script\_donotdelete/all\_db\_down\_alert\_email.ksh

######## Listener Down Alert Report ##############################

\*/10 \* \* \* \* /opt/workspace/listener\_down\_script\_donotdelete/listener\_status\_sliusedorasq50.ksh

\*/10 \* \* \* \* /opt/workspace/listener\_down\_script\_donotdelete/all\_listener\_down\_alert\_email.ksh

######## Level 0 Backup ##########

0 19 \* \* 0-6 /opt/oracle/scripts/FULL\_BKP.sh dctm2dv

0 22 \* \* 0-6 /opt/oracle/scripts/FULL\_BKP.sh dctm2ts

0 1 \* \* 0-6 /opt/oracle/scripts/FULL\_BKP.sh glims2qa

0 5 \* \* 0-6 /opt/oracle/scripts/FULL\_BKP.sh glims2dv

####### Level 1 Incremental Backup #############

#0 1 \* \* 1-6 /opt/oracle/scripts/INC\_BKP.sh dctm2dv

#0 2 \* \* 1-6 /opt/oracle/scripts/INC\_BKP.sh dctm2ts

#0 3 \* \* 1-6 /opt/oracle/scripts/INC\_BKP.sh glims2qa

#0 4 \* \* 1-6 /opt/oracle/scripts/INC\_BKP.sh glims2dv

####### Archive Log Backup ###########

0 \*/4 \* \* \* /opt/oracle/scripts/ARC\_BKP.sh dctm2dv

0 \*/4 \* \* \* /opt/oracle/scripts/ARC\_BKP.sh dctm2ts

0 \*/4 \* \* \* /opt/oracle/scripts/ARC\_BKP.sh glims2qa

0 \*/4 \* \* \* /opt/oracle/scripts/ARC\_BKP.sh glims2dv

####### Monthly Full Backup Backup ###########

#0 2 1 \* 0 /opt/oracle/scripts/MONTHLY\_FULL\_BKP.sh dctm2dv

#0 4 1 \* 0 /opt/oracle/scripts/MONTHLY\_FULL\_BKP.sh dctm2ts

#0 23 1 \* 0 /opt/oracle/scripts/MONTHLY\_FULL\_BKP.sh glims2qa

#0 20 1 \* 0 /opt/oracle/scripts/MONTHLY\_FULL\_BKP.sh glims2dv

#25 9 \* \* \* sh /opt/oracle/scripts/FULL\_BKP\_dctm2dv.sh

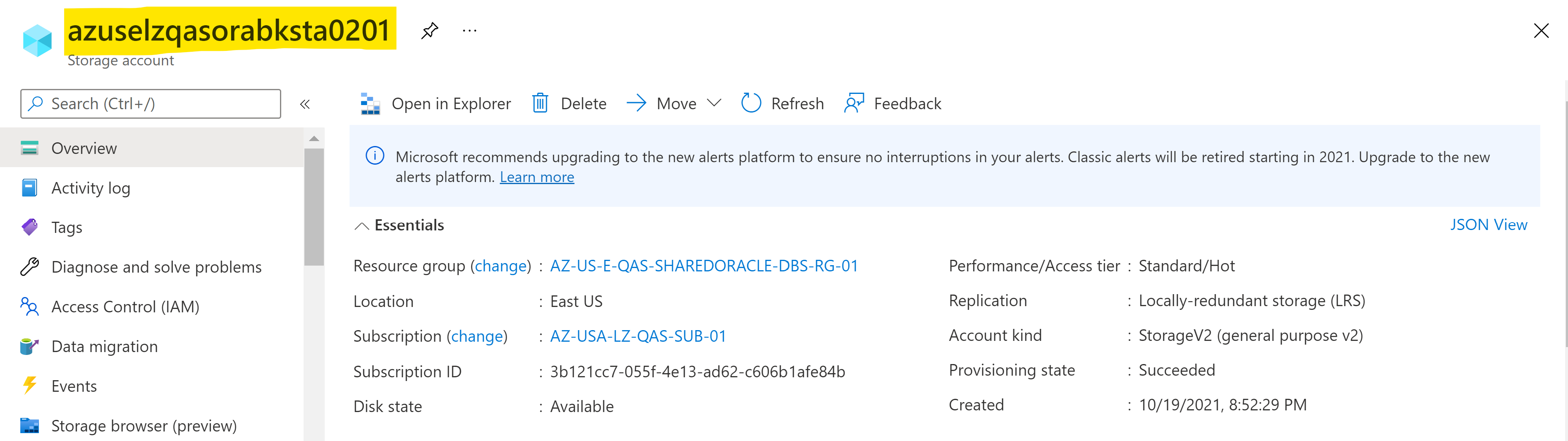
#16 10 \* \* \* /opt/oracle/scripts/FULL\_BKP.sh dctm2dv

1. Configuring and Mounting Storage account

The RMAN backups are written onto the storage account and the storage account is mounted using “blobfuse”. The storage account is mounted on the VM as “/rmanbackup”.

* + 1. Storage Account and Private Endpoints

Storage account is created with private endpoints and private DNS zone.



Graphical user interface, application

Description automatically generated

Graphical user interface, text, application, email

Description automatically generated

* + 1. Mounting storage account using “blobfuse”

The storage account is mounted on the VM using [blobfuse](https://docs.microsoft.com/en-us/azure/storage/blobs/storage-how-to-mount-container-linux).

1. RMAN Backup Retention Policy
   * 1. Storage Account Lifecycle Management

RMAN backups are written to the storage account/container. The [Lifecycle Management](https://docs.microsoft.com/en-us/azure/storage/blobs/lifecycle-management-overview) from storage account is used to manage the backups. The storage account is created with access tier as “Hot” (which means data is accessed frequently). Using the Lifecycle Management, the blobs (data in the containers) can be moved to “Cool” or “Archive” tiers. The “Cool” or “Archive” tiers are inexpensive options of storage compared to ‘Hot” tier. Example of policy below.

**Note**: Once the blobs are converted to “Cool” or “Archive” they need to be converted back to “Hot” tier to access them or use them for restorations.

Graphical user interface, text, application, email

Description automatically generated

Graphical user interface, text, application

Description automatically generated

Graphical user interface, text, application, email

Description automatically generated Graphical user interface, application

Description automatically generated